2012-2013 Annual Report

Saskatchewan
Information and
Privacy Commissioner

Saskatchewan
Information and Privacy
Commissioner

503 - 1801 Hamilton Street
Regina, Saskatchewan
S4P 4B4

Tel: (306) 787-8350
Fax: (306) 798-1603
Website: www.oipc.sk.ca

June 21, 2013

Hon. D. D'Autremont
Speaker of the Legislative Assembly
129 Legislative Building
Regina, Saskatchewan
S4S 0B3

Dear Mr. Speaker:

I have the honour to present to the Legislative Assembly my 2012-2013 Annual Report in accordance with the provisions of section 62(1) of *The Freedom of Information and Protection of Privacy Act,* section 52(1) of *The Local Authority Freedom of Information and Protection of Privacy Act* and section 60(1) of *The Health Information Protection Act.*

Respectfully submitted,

R. Gary Dickson, Q.C.
Saskatchewan Information and Privacy Commissioner

In short, Mr. Speaker, the people of Saskatchewan trust their health professionals to handle their personal health information with respect for their right to personal privacy. The people of Saskatchewan deserve no less.

...

That is why, Mr. Speaker, *The Health Information Protection Act* is so important. It ensures that even in the fast moving health system of today the tradition of respecting individual privacy will continue into the future. In fact, Mr. Speaker, we believe that this new important legislation adds significantly to the protection we have all come to expect from the health system.

Mr. Speaker, *The Health Information Protection Act* is about the rights of individuals to protect their personal health information. The Act enshrines in legislation certain rights that every person in this province has in regard to their personal health information.

Hon. Ms. Junor to move second reading of Bill 29 – *The Health Information Protection Act* on April 26, 1999 (*Hansard* p. 761)

The [Freedom of Information and Protection of Privacy] Act's basic purpose reflects a general philosophy of full disclosure unless information is exempted under clearly delineated statutory language. There are specific exemptions from disclosure set forth in the Act, but these exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act.

Mr. Justice Tallis, Saskatchewan Court of Appeal, General Motors Acceptance Corporation of Canada v. Saskatchewan Government Insurance, 1993, SJ No. 601, at paragraph [11].

Table of Contents

Introduction 1

Commissioner's Message 3

OIPC Organizational Chart 8

Detailed Research and Commentary 9

Communication and Education 10

The Health Information Protection Act 16

The Freedom of Information and Protection of Privacy Act 46

The Local Authority Freedom of Information and Protection of Privacy Act 56

National Freedom of Information Audit 2012 58

Open Government - Open Data 59

Case Report Summaries 60

Financial Statements 84

Appendices 94

Introduction

The role of the Information and Privacy Commissioner has sometimes been described as that of the umpire in the information age.

That role has also been described as follows:

> Our recent comparative analysis of privacy protection policy has concluded that, regardless of legislative powers, every data-protection commissioner in Canada and elsewhere is expected at some point to perform seven interrelated roles: ombudsman, auditor, consultant, educator, policy adviser, negotiator, and enforcer.
>
> Colin J. Bennett, "The Privacy Commissioner of Canada: Multiple Roles, Diverse Expectations and Structural Dilemmas," *Canadian Public Administration* Volume 46, Issue 2 (June 2003)

In 1992, *The Freedom of Information and Protection of Privacy Act* (FOIP) was proclaimed. This enshrined two principles:

1. public records must be accessible to the public; and
2. "personal information" must be protected by public bodies.

FOIP applies to all "government institutions". This captures all Ministries of the Saskatchewan Government plus Crown corporations, Boards, Commissions and Agencies.

In 1993, *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) was proclaimed. This law is very similar to FOIP, but applies to "local authorities" such as schools, universities, regional health authorities, municipalities, and library boards.

In 2003, *The Health Information Protection Act* (HIPA) was proclaimed. This applies to organizations and individuals designated as a health information "trustee", defines what is "personal health information" and sets the rules for how that personal health information can be collected, used and disclosed. It also provides a right of access to personal health information and a right to seek correction of errors.

The Supreme Court of Canada has declared that laws like FOIP, LA FOIP and HIPA are special kinds of laws that define fundamental democratic rights of citizens. They are "quasi-constitutional" laws that generally are paramount to other laws.

The Supreme Court of Canada has declared that laws like FOIP, LA FOIP and HIPA are special kinds of laws that define fundamental democratic rights of citizens (Gérard V. La Forest, *The Offices of The Information and Privacy Commissioners: The Merger and Related Issues*, November 15, 2005, p. 8). They are "quasi-constitutional" laws that generally are paramount to other laws.

Mandate of the Commissioner

There are four major elements in the Saskatchewan Information and Privacy Commissioner's mandate defined by FOIP, LA FOIP and HIPA:

1. The Commissioner responds to requests for review of decisions made by government institutions, local authorities or trustees in response to access requests, and makes recommendations to those bodies.

2. The Commissioner responds to complaints from individuals who believe their privacy has not been respected by government institutions, local authorities or trustees, and makes recommendations to those bodies.

3. The Commissioner provides advice to government institutions, local authorities or trustees on legislation, policies or practices that may impact citizens' access or privacy rights.

4. The Commissioner provides education with respect to information rights including both access to information and protection of privacy.

Mission Statement

The people of Saskatchewan shall enjoy the full measure of information rights that have been affirmed by the Legislative Assembly of Saskatchewan.

Vision

Saskatchewan government institutions and local authorities operating in a fashion that is as transparent as possible and with the greatest sensitivity to the privacy of the people of Saskatchewan, all in accordance with the provisions of the applicable legislation.

Saskatchewan health information trustees operating in a fashion that fully respects the privacy rights of the people of Saskatchewan guaranteed by *The Health Information Protection Act* and the *Canadian Charter of Rights and Freedom*.

OIPC Values

Integrity

Responsibility & Accountability

Excellence

Respectful Workplace

Promote Knowledge

Commissioner's Message

R. Gary Dickson, Q.C.
Saskatchewan Information and Privacy Commissioner

This is my final Annual Report since my second term as Saskatchewan Information and Privacy Commissioner will end April 27, 2014.

I want to express my appreciation and my profound respect for the team that I have worked with for the last nine years. They have been resourceful, skilled and dedicated to promoting the access and privacy rights of Saskatchewan citizens. Jurisdictions as distant as Mexico and a number of nations in East Africa have sought advice from our office on how we leverage small resources to create greater awareness of access and privacy rights. Unfortunately, too much attention is paid to the person who occupies the position of Commissioner and far too little recognition is afforded the individuals who do so much of the heavy lifting.

In the last nine years, our Portfolio Officers have generated 75 formal access and privacy reports, opened 1,322 case files and closed 1,235 of them. We have continually added resources to our website (www.oipc.sk.ca) that last year attracted 1,465,958 hits and 94,294 visits of longer duration. This team has developed more than 40 different resources for public bodies, trustees and the public; all of them are available on our website. We have archived on our website 94 issues of our e-newsletter, the *Saskatchewan FOIP FOLIO*. Each year our Portfolio Officers respond to approximately 3,000 requests by phone and email for advice about the laws we oversee and the process to make a privacy complaint, request access or appeal to this office. Our office has supported the annual Right to Know Week for each of the last seven years. We have undertaken more than 1,000 education presentations in some 34 different Saskatchewan communities. Each of these reports, newsletters and resources could be said to bear the fingerprints of virtually everyone on our team. I am very proud of each member of the team and am confident that the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) will continue to be an effective and respected agency of its kind in Canada.

It would be hard to imagine how any province could develop a robust access and privacy culture when it had only a part-time Information and Privacy Commissioner with no staff, no dedicated access and privacy unit to lead FOIP compliance throughout Executive Government and virtually no dedicated resources to the mission. Yet that describes the situation from 1992 when the law was proclaimed until the decision of the Legislative Assembly (the Assembly) in 2003 to hire a full-time Information and Privacy Commissioner and provide resources including staff to meet what is a very broad mandate.

Although this province has a considerable distance to go to develop the kind of access and privacy culture evident in Alberta and British Columbia, Saskatchewan certainly has made considerable progress in the last nine years. Many of those highlights were listed in my last Annual Report which celebrated the 20th anniversary of FOIP in Saskatchewan.

We can easily see increased activity throughout the province with more citizens making access requests, heightened awareness among health care professionals of their responsibilities to protect patient information and more consideration by public sector organizations when they contemplate new programs that impact the information rights of citizens. Much of this Annual Report is devoted to assessing HIPA compliance ten years after it was proclaimed.

My observation is that in 2012-2013 some of the momentum that was evident in Saskatchewan in the early years of my first term as Commissioner appears to have stalled. The Ministry of Justice, Access and Privacy Branch, was created in 2005-2006 but has not expanded significantly even as the volume of access requests across government has increased. The OIPC grew steadily in the early years from two permanent full-time employees to eight permanent full-time employees (including the Commissioner) but my requests for a fourth Portfolio Officer or investigator have now been denied by the Board of Internal Economy for six consecutive years. The Health Ministry, which has administrative responsibility for HIPA, appears to have lost some of its focus on providing both trustee organizations and patients with tools and resources to navigate HIPA. Ministries are introducing proposed legislation to the Assembly which could have benefited from more careful analysis of existing access and privacy laws and how these Bills will impact the information rights of citizens. More public sector organizations could benefit from undertaking a thorough Privacy Impact Assessment (PIA) before they implement new programs and policies that will impact citizens' access and privacy rights. Our encouragement for legislative updating of FOIP, LA FOIP and HIPA has been ignored for the last nine years.

What is the impact on the people of Saskatchewan when the Government of Saskatchewan's work in building a robust access and privacy regime stalls? You could be the individual who spent six years fighting to get access to records about him from the Ministry of Justice and who was met with apparent indifference and unconscionable delays (Review Report F-2012-006). You could be the employee in a regional health authority who could not understand why details of his salary would be published on the internet with no attempt being made, by the use of simple privacy enhancing technology, to minimize the risk of data profiling. (Investigation Report LA-2012-002). You could be the patient who could not get a copy of their own personal

health information from their health care professional (Review Reports H-2008-002, H-2008-001, H-2007-001). You could be the patient who learns that your entire patient file with information about your lab tests, diagnostic tests, drug profile, psychiatric history, clinical notes and health history was carelessly tossed into a recycling bin (Investigation Report H-2011-001). You could be the citizen attempting to obtain records about a contract your local school division entered into with a taxi company which would be paid with public funds (Review Report LA-2012-004). You could be the citizen wanting to see some of the statistical and historical information assembled by government officials to provide background information to new Cabinet Ministers but which took approximately five years to get to the report stage (Review Report F-2012-004). Even when Executive Council agreed, following our Report, to provide the Applicant with the kinds of information recommended for release, Executive Council insisted for the first time that the applicant must pay $1,750 before this material would be made available to him. You could be an injured worker attempting to see records the Saskatchewan Workers' Compensation Board has about you but which it refuses to provide since it asserts that it does not have the same obligations of operating transparently that every other provincial government institution and local authority in Saskatchewan must follow (Review Report F-2012-005). You could be an employee of a regional health authority who discovered that another employee snooped in your electronic health record, deleting some information and inserting some defamatory information all without your knowledge or consent (Investigation Report H-2013-001).

My question for the Members of the Legislative Assembly would be: Why should these constituents not be able to enjoy the same rights that their neighbours in Alberta and British Columbia take for granted? And the further obvious question: Why should Saskatchewan public bodies and trustees not be held to the same degree of accountability as similar institutions in other provinces?

So, what do the citizens in the provinces of Alberta and British Columbia have that Saskatchewan residents are missing? I would suggest the features in those jurisdictions include:

- In those provinces, there is an explicit duty on all public bodies to take appropriate measures to protect the personal information entrusted to them. This statutory duty is reinforced by an offence provision and substantial penalties for non-compliance. Not in Saskatchewan.

- In those provinces, employees who work in the private sector for businesses such as the car dealership, the grocery store and the law firm or accounting

firm have the same privacy protection available to anyone who works in the public sector. Not in Saskatchewan.

- In those provinces, the rules by which citizens can make access requests and request that breaches of their privacy be investigated are consolidated in a single statute which applies to Ministries, Crown corporations but also schools, hospitals, municipalities, universities and colleges. Not in Saskatchewan where we have the confusion of two different laws, two different sets of forms, and different approaches to fees.

- In those provinces, you have the right to make an access request to your municipal police service just as you would with any other public sector body in Alberta or British Columbia. Not in Saskatchewan.

- In those provinces, you have the right to make an access request to Saskatchewan Workers' Compensation Board for any recorded information in the possession or under the control of Saskatchewan Workers' Compensation Board. Not in Saskatchewan.

- In those provinces, there is a public interest override that imposes a positive duty on the head of a public body to disclose information to the public where there is a significant risk of injury or harm to the public. This duty operates regardless of whether a formal access request has been made. This serves to provide some balance to the long list of exemptions in each province's access law that allow access to be denied. Not in Saskatchewan.

- In those provinces, you are not obligated to rely on guidance from the Ministry of Justice when you are trying to understand and to utilize the access and privacy law, since the Ministry of Justice provides legal advice for all ministries. Lawyers from the Ministry of Justice are usually focused on the parochial interests of the client ministry and may not always be sufficiently mindful of the larger objective of enhanced transparency to citizens. In those provinces, administrative responsibility is assigned to a different Ministry and usually one that provides a range of services to the public and which has no stake in access and privacy reviews other than to ensure the applicable law is followed in the spirit of promoting transparency. Not in Saskatchewan.

- In those provinces, the access and privacy laws that were proclaimed in 1993 (British Columbia) and in 1995 (Alberta) have been reviewed several times in a public process by all-party committees of Members of their Assembly to

address changed circumstances, new privacy risks and to improve their third generation laws. A significant number of changes have been made to both provinces' laws to ensure a better job is done for citizens and public bodies alike. Not in Saskatchewan where our law is based on a 30 year old model and has never been significantly revised in the 21 years it has been in force. There is no requirement for a statutory review of any of FOIP, LA FOIP or HIPA as is the case in both British Columbia and Alberta.

- In those provinces, the oversight is provided by Information and Privacy Commissioners who focus on informal resolution of complaints but who also have the power to issue binding orders to require a public body to do something or cease doing something and these orders can be enforced like a court order. Not in Saskatchewan.

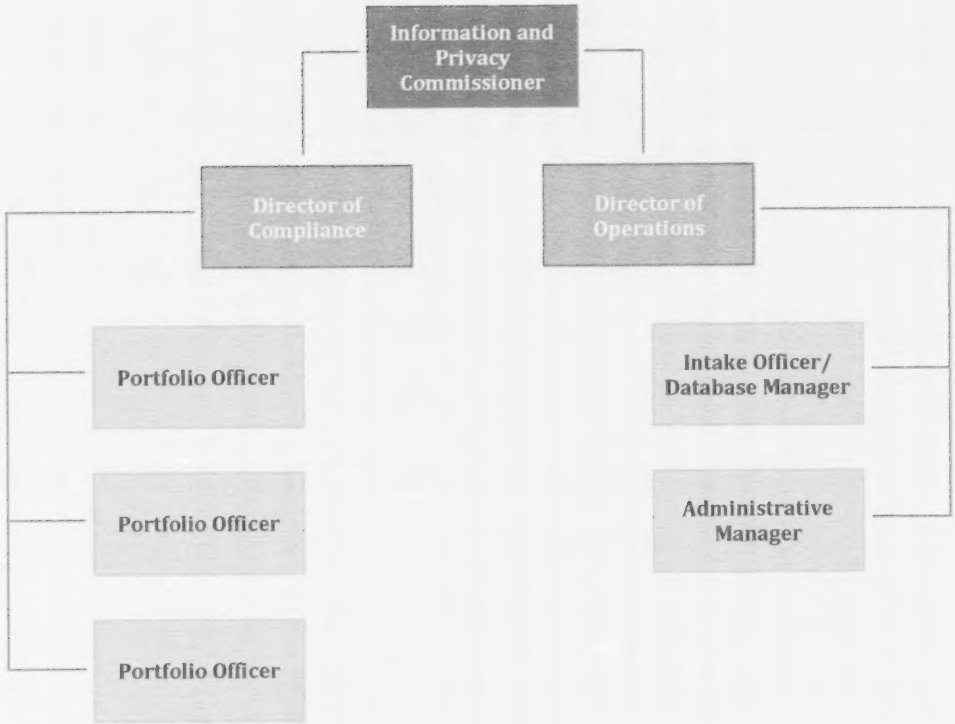
- Every citizen in those provinces has free access to a large, comprehensive manual developed by professional communicators to unravel the mysteries of access and privacy law complete with examples, references to Commissioner Orders, checklists, decision 'trees' and charts available online. This resource explains each of the mandatory and discretionary exemptions and how to apply them. Not in Saskatchewan.

- In those provinces, a very ambitious campaign was developed before the access and privacy laws came into force to build public awareness of the laws and to ensure that all public sector employees would have a good understanding of those laws and their obligations under them. This has been supplemented with first class educational materials, in-service training and a large number of resources, many of which have been co-branded by the Government and by the Office of the Information and Privacy Commissioner. Not in Saskatchewan.

When it comes to access and privacy, Saskatchewan is still a have-not province.

Gary Dickson
Saskatchewan Information and Privacy Commissioner

OIPC Organizational Chart



Detailed Research and Commentary

We continue to receive requests for advice and assistance from government institutions, local authorities and trustees which are considering new legislation, regulations, policies or programs that will or may affect the access and privacy rights of Saskatchewan citizens. We view such requests as a positive development since it indicates a wish to ensure full compliance with the applicable law. We advise these organizations that we cannot provide any kind of advance ruling but that we will provide them with general, non-binding advice. We offer to provide this advice on a confidential basis but with the caveat that if the particular initiative of that organization proceeds with what we consider deficient provisions to deal with access or privacy rights, we may provide public commentary on our website outlining those deficiencies. We consistently encourage public sector organizations and trustees to 'bake in' strong access and privacy features from the earliest design stage of any new initiative that involves access to information and privacy.

A significant number of programs, Bills, regulations and policies are implemented without any prior consultation with our office. Many of these initiatives involve extensive sharing of personal information of citizens with multiple public bodies, trustees and often bodies that are not even covered by our provincial access and privacy laws. Many of these initiatives would have benefited significantly by prior consultation with the OIPC since it is usually much more difficult to make revisions after the law has been passed or the program rolled out.

An excellent example would be the provision in Bill 65 - *The Securities Amendment Act, 2012*, which received first reading in the fall of 2012 and which erroneously states that corporations have a right of privacy in Saskatchewan. This is an obvious error that should have been caught prior to the Bill being printed. As well, on the merits of the Bill, the draftspersons apparently did not consider three other surgical options which may have achieved the purpose of the Bill and yet avoided the need for the blunt technique of exclusion from FOIP.

A tool that we ask public bodies and trustees to use prior to seeking our assistance is the PIA. This form is available on our website for each of the three statutes that we oversee.

A tool that we ask public bodies and trustees to use prior to seeking our assistance is the PIA. This form is available on our website for each of the three statutes that we oversee.

A tool that we ask public bodies and trustees to use prior to seeking our assistance is the PIA. This form is available on our website for each of the three statutes that we oversee. The PIA will help to identify shortcomings and problem areas and also provide clarity for public bodies and trustees which are considering new policies and procedures in their respective offices.

Communication and Education

Public Emergency Response

The OIPC has been in discussion with other oversight offices with respect to an initiative of the Privacy Commissioner of Canada. After the New Zealand earthquake, important lessons about privacy issues and information sharing informed the work of the New Zealand Privacy Commissioner. These lessons have been considered in Canada and have led to a comprehensive information kit assembled by the Privacy Commissioner of Canada. There is a hyperlink on our website, www.oipc.sk.ca to the federal information kit. Our website offers some related materials that consider the specific provisions in FOIP, LA FOIP and HIPA that would enable necessary information sharing in the event of a public emergency that puts at risk many citizens, and requires a quick and appropriate response by government agencies and public sector bodies.

Our website offers some related materials that consider the specific provisions in FOIP, LA FOIP and HIPA that would enable necessary information sharing in the event of a public emergency...

OIPC Communication Projects

In the last year we produced another ten issues of our e-newsletter, the *Saskatchewan FOIP FOLIO*. This continues to be an effective means of alerting members of Saskatchewan's burgeoning access and privacy community, and FOIP Coordinators in particular, to new access and privacy developments in our province and beyond. This publication informs subscribers of new tools and resources created by our office or by others that may be helpful. It also alerts them to new Investigation Reports and Review Reports from our office.

Our website continues to be a useful communication tool for the public and those organizations we oversee. In 2012-2013, our site, www.oipc.sk.ca attracted more than 1.4 million hits. In this past year, the website attracted 94, 294 'visitors' who stayed on our site longer and viewed more pages on the website.

One of the most important services that we provide is summary advice when we get inquiries about access and privacy and the three statutes that this office oversees. This last fiscal year we received 2,907 of such inquiries.

We also provided 75 presentations on one or more of the three laws that we oversee to a variety of audiences in a number of Saskatchewan communities. A sample of such presentations is included as Appendix 4.

Now that we have 75 case reports on our website, our *Annotated Section Index* for each of the three laws becomes more useful.

Your Information Rights (Access to Information and Protection of Privacy)

You have the right to make an access to information request for information in any recorded form or format (paper or electronic records) in the possession/custody (on premises, etc.) or control (off site, in contractor's possession, etc.) of a government institution (i.e. Ministries, Crown corporations, boards, commissions and agencies), local authority (i.e. school and library boards, regional health authorities, municipalities, etc.) and/or trustee organization (i.e. clinic, dentist, pharmacy, etc.).

To make a request, please see the steps listed on page 14.

You have the right to request correction or amendment to records that the above noted organizations hold if you believe they contain errors or omissions.

That process is as follows:

- Start by making an access to information request to receive a copy of the record(s).
- Next, make a formal request in writing to the organization requesting correction or amendment.
- The organization will then make the change or add a notation that the request was made but it chose not to alter for whatever reasons.
- If dissatisfied, request that we undertake a review of the organization's decision.

You have the right to complain to the Information and Privacy Commissioner if you believe the organization in question has breached your privacy. We are an appeal body, so you must first deal with the organization in question.

To make a privacy complaint, please see the steps listed on page 15.

Your personal information is information of a personal nature about you and is defined by FOIP and LA FOIP. Personal health information is defined by HIPA and has more to do with your health and health related services. It is not considered personal information or personal health information if sufficiently de-identified. Also, business card information and work product is generally not considered to be personal information.

You have a measure of control over what these organizations do with your personal information and/or personal health information but, as they provide services for your benefit (i.e. health care, education, social services), often your consent is not required for the sharing of your information to occur as long as it is otherwise authorized by law. However, you should be informed why your information is needed and how it will be used (notice requirements). If you have questions about what personal information or personal health information is collected or how it is being used or otherwise shared, you may contact the organization's FOIP Coordinator or Privacy Officer to discuss.

If for some reason you do not want your information shared, you can ask the trustee organization not to share details of recent health services received with your immediate family or persons to whom you have a close personal relationship. Without this instruction, limited information regarding your personal health information may be shared by the trustee with family and friends without your consent.

You have the right to designate another person or 'surrogate' in writing to exercise your rights or powers under these three laws. For instance, you can provide written authorization for someone to make an access request on your behalf. It does not have to be a relative.

At present, you cannot 'opt out' of the electronic health record; however, you can request that eHealth Privacy Service 'globally' mask your personal health information profile in the following: the Pharmaceutical Information Program, the Picture Archiving and Communication System and/or the Saskatchewan Laboratory Results Repository. For more information on this service, contact eHealth Privacy Service.

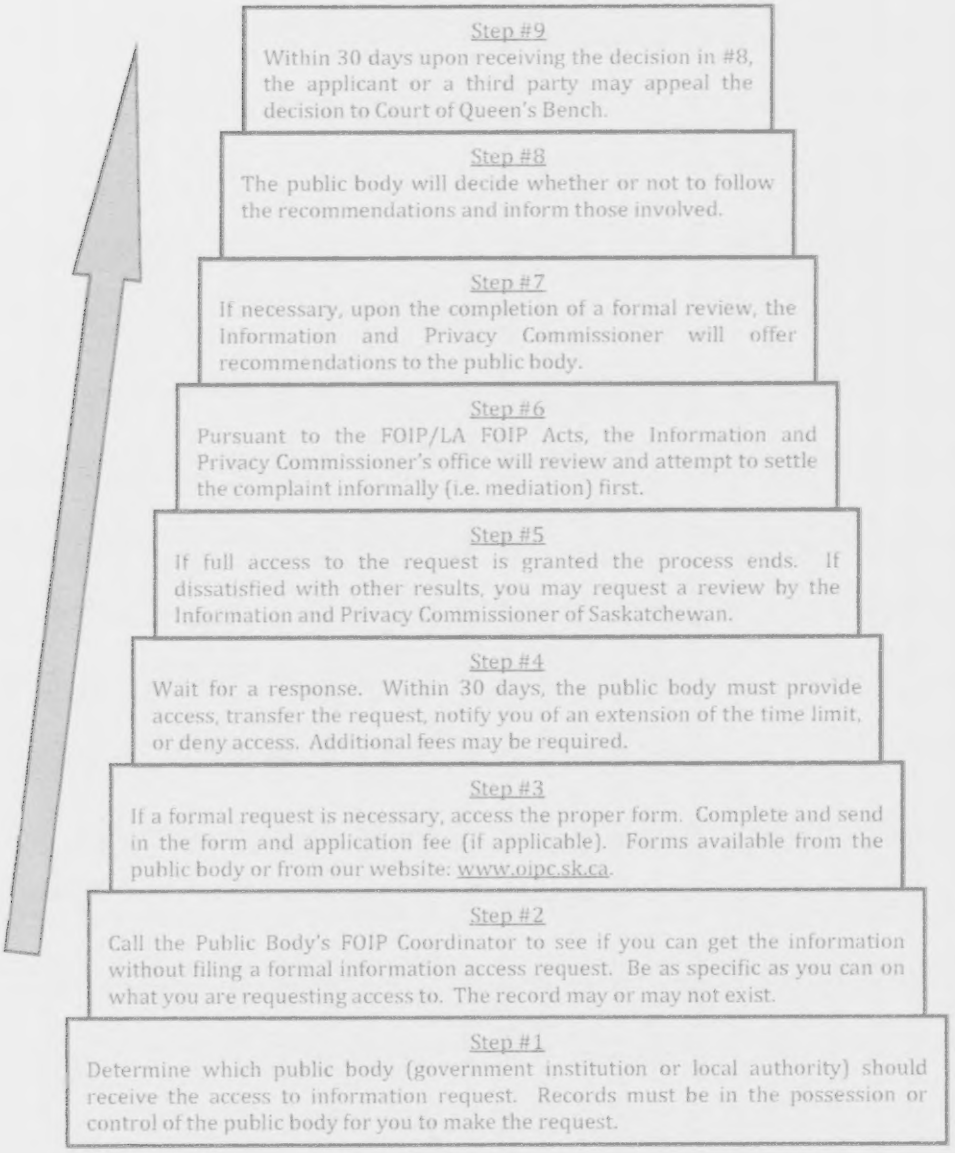
As the province adds components to its expanding electronic health record, you now have the ability to see what is contained within each data repository (i.e. medication profile print-out, diagnostic images and lab results), but you also have the right to see which health care worker or professional has viewed your personal health information in any specified time period.

In order to request a copy of either report, contact the following:

eHealth Privacy Service
Suite 360, 10 Research Drive
Regina, SK S4S 7J7
Phone: 1-800-667-1672
Email: privacyandaccess@ehealthsask.ca

How to Make an Access Request

The Freedom of Information and Protection of Privacy Act (FOIP) & *The Local Authority Freedom of Information and Privacy Act* (LA FOIP)


Step #9
Within 30 days upon receiving the decision in #8, the applicant or a third party may appeal the decision to Court of Queen's Bench.
Step #8
The public body will decide whether or not to follow the recommendations and inform those involved.
Step #7
If necessary, upon the completion of a formal review, the Information and Privacy Commissioner will offer recommendations to the public body.
Step #6
Pursuant to the FOIP/LA FOIP Acts, the Information and Privacy Commissioner's office will review and attempt to settle the complaint informally (i.e. mediation) first.
Step #5
If full access to the request is granted the process ends. If dissatisfied with other results, you may request a review by the Information and Privacy Commissioner of Saskatchewan.
Step #4
Wait for a response. Within 30 days, the public body must provide access, transfer the request, notify you of an extension of the time limit, or deny access. Additional fees may be required.
Step #3
If a formal request is necessary, access the proper form. Complete and send in the form and application fee (if applicable). Forms available from the public body or from our website: www.oipc.sk.ca.
Step #2
Call the Public Body's FOIP Coordinator to see if you can get the information without filing a formal information access request. Be as specific as you can on what you are requesting access to. The record may or may not exist.
Step #1
Determine which public body (government institution or local authority) should receive the access to information request. Records must be in the possession or control of the public body for you to make the request.

How to Make a Privacy Complaint

1. The Complainant should first contact the Privacy Officer or FOIP Coordinator for the government institution, local authority or trustee to attempt to resolve the complaint.

   If no satisfactory resolution of the concern is reached by dealing directly with the public body, the Complainant may choose to file a written complaint with the Information and Privacy Commissioner.

2. The complaint should be in writing and should provide the following:

   - Date;
   - Complainant's name, address and phone number;
   - Specific government institution, local authority or trustee against whom the complaint is made;
   - Copies of any correspondence with the public body relevant to the complaint;
   - Description of the events giving rise to the complaint; and
   - Clarify whether the Complainant wishes to be treated anonymous when the OIPC communicates with the public body.

3. Once we review the complaint the following will occur:

   - Once it is determined that the OIPC has jurisdiction to investigate, a Portfolio Officer will be assigned to the file.
   - The Portfolio Officer will advise the public body of the complaint and that the OIPC will be investigating under the authority of FOIP, LA FOIP or HIPA. At the same time, we will advise the Complainant that an investigation is underway.
   - The Portfolio Officer will gather information from the public body to determine the relevant facts.
   - The Portfolio Officer will define the issues for purposes of the investigation and invite submissions from the public body and the Complainant.
   - The Portfolio Officer will attempt to mediate, or otherwise informally resolve the complaint, with complainant and public body.
   - If no meditated settlement is possible, the Commissioner will proceed to issue a formal Investigation Report. The identity of the complainant will not be disclosed.
   - There may be a limited right of appeal to the Court of Queen's Bench by an aggrieved complainant if the complaint was handled under HIPA pursuant to section 42(1)(c). No right of appeal from a Report dealing with a breach of privacy under FOIP or LA FOIP.

The Health Information Protection Act

Marking the 10th Anniversary of *The Health Information Protection Act*

Background

The purpose of HIPA was to facilitate the creation of the electronic health record for every man, woman and child in this province. In fact, the announcement that the Saskatchewan Government of the day would introduce a new Bill – *The Health Information Protection Act* was in the same paragraph of the March 9, 1998 Throne Speech as the announcement of the Saskatchewan Health Information Network.

Saskatchewan Health Information Network's purpose, as a Crown corporation, was to build the province's electronic health record system. It was evident in the speeches of the then Minister of Health and representatives of the Government in 2003 that there was important direct linkage between the electronic health record and HIPA. Although HIPA also applies to all personal health information in paper records as well as electronic records in the custody or under the control of a trustee, it was specifically designed to enable electronic health records.

HIPA represented a significant change to the operations of health care providers and certainly impacted the relationship between patients and their Saskatchewan providers.

HIPA represented a significant change to the operations of health care providers and certainly impacted the relationship between patients and their Saskatchewan providers.

HIPA has had an interesting genesis. It was an initiative similar to initiatives in the late 1990s in Manitoba and Alberta. It represented an unusual confluence of trends and priorities. There were recommendations from auditors for better information for purposes of health care planning and investment to optimize the value for those public funds going to health care. Technology, including electronic health records, was seen as an important measure to create more efficiency in health care delivery and to control costs. There was a federal Advisory Council on Health Infostructure considering an electronic health record system in 1998 and 1999. It's final report "Paths to Better Health" in February 1999 advocated a Canada Health Infoway that would become "the key information and communication foundation for our health care system in the 21st century".

At the same time, there was a sharper focus on privacy by reason of the European Union (EU) Data Protection Directive of 1995 that put at risk Canada's international trade with the European Union and its member nations unless Canada enacted legislation "substantially similar" to the Fair Information Practices developed by the Organization for Economic Cooperation and Development (OECD). This led to the enactment of the *Personal Information Protection and Electronic Documents Act* in 2001. The *Personal Information Protection and Electronic Documents Act* was being developed by Industry Canada, at about the same time that the policy decision was made in each of those three prairie provinces to implement a system of electronic health records for all citizens. HIPA was introduced in the Assembly in 1998, it attracted Royal Assent in 1999 but was not proclaimed until amendments were made in 2003. HIPA was proclaimed September 1, 2003.

There was a limited public consultation in 1998 reflected in the *Consultation Paper on Protection of Personal Health Information*. This report prepared by Saskatchewan Health identified a number of significant privacy concerns raised by those surveyed in the course of the consultation. These included:

There was a limited public consultation in 1998 reflected in the *Consultation Paper on Protection of Personal Health Information*. This report prepared by Saskatchewan Health identified a number of significant privacy concerns raised by those surveyed in the course of the consultation.

- 81.4% agreed that "...responsibility for the record should remain with the doctor, hospital, or whoever is closest to the client/provider relationship, not with a central agency managing data collection."

- "95% indicated agreement with the statement: the individual has rights to access her or his own information and has some control over what happens to that information."

- "90% had some level of agreement that: Wherever possible and practical, information about individuals should be collected directly from the individual the information is about."

- "83.5% had some agreement with the statement that: Individuals, in certain circumstances, should have the right to refuse to give certain information or to limit its use."

There were some particular challenges with the roll-out of HIPA. One was that Saskatchewan did not have a mature access and privacy regime in 2003. *The Freedom of Information and Protection of Privacy Act* (FOIP) had applied to the Ministry of Health since 1992. *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) applied to regional health authorities since 1994. For a number of reasons, there was little familiarity with the legislation, very few access requests,

little guidance on how to respond to access or correction requests, extremely limited experience with privacy regulation and only a part-time Information and Privacy Commissioner. Although the mandate for the Commissioner under FOIP and LA FOIP was very broad, without an office, staff and significant budget, only the reactive portions of the mandate could be addressed by the three successive part-time Commissioners.

For HIPA, the Ministry of Health apparently did not have a comprehensive plan for education of trustees. There was confusion within the Government as to the impact of the *Personal Information Protection and Electronic Documents Act*, which was to come into force in its full scope on January 1, 2004, and the decision was made to proclaim HIPA before the *Personal Information Protection and Electronic Documents Act* came into force although that also meant before adequate preparations had been made for its implementation.

This decision perhaps accounts for the peculiar announcement from the Ministry of Health to trustees in the summer of 2003. This was the announcement that HIPA would be proclaimed September 1, 2003 but that there would be a grace period and no enforcement action taken under HIPA during the grace period. There were two significant problems with that announcement. First, there was no end date to the so called grace period, so the incentive for trustee organizations to quickly put in place the necessary tools and resources and training for compliance was absent. Second, the Ministry of Health's role under HIPA was responsibility for administration of HIPA not enforcement which is assigned by HIPA to the independent officer of the Legislative Assembly – the OIPC and the Court of Queen's Bench. The OIPC is to investigate denial of access to patients and breaches of privacy. If a patient is dissatisfied with a trustee's response to OIPC recommendations, that patient can appeal to the Court. If prosecution is to be initiated, approval of the Minister of Justice is essential. It was not the Ministry of Health's role to unilaterally create a grace period.

The other significant decision was to not hire outside health privacy expertise to assist preparing the Ministry of Health and the large institutional trustees such as the Saskatchewan Cancer Agency, regional health authorities and the regulatory colleges for compliance. This should have included the preparation of a comprehensive, accessible manual for HIPA. I discussed this in my *2004-2005 Annual Report* (page 35). The chosen approach in Saskatchewan, however, was to require each of these large trustee organizations to nominate someone as the Privacy Officer and task them to become part of the Chief Information Officer Forum's Security and Privacy sub-committee which would draft the policies and procedures contemplated by section 16 of HIPA. The Ministry of Health arranged for legal advice to the sub-committee from a

law firm. There was both a lack of leadership and a lack of health privacy experience that translated into delays of many years in development of policies and procedures. The relationship to the full-time OIPC was also quite unlike the collaboration happening in both Manitoba and Alberta. The OIPC was not involved with the sub-committee developing the policies and procedures. In the result, occasionally the OIPC would be presented with various materials produced by the sub-committee that we would determine were inaccurate and not appropriate. The sub-committee would then have to redo their materials which in turn translated into more delay.

The original scheme was to assign responsibility for the development of the electronic health record to a new Crown corporation, namely Saskatchewan Health Information Network. Subsequently, the Health Information Solutions Centre was created within the Ministry of Health and assumed this responsibility. Then in late 2011, eHealth Saskatchewan was created as a Crown corporation with the mandate to design and implement the electronic health record. Effectively, the Health Information Solutions Centre was transferred to eHealth Saskatchewan with a new Chief Executive Officer but a similar mandate. I will consolidate most of my commentary with respect to the electronic health record in the later section of the Annual Report dealing with *eHealth Saskatchewan.*

I cite this history summary of HIPA since it may explain in part some of the implementation difficulties that this province has experienced for the first decade of HIPA. I might also note that, unlike the other western provinces with a stand-alone health information law, this province refused to endorse the *Pan Canadian Health Information Privacy and Confidentiality Framework.* As noted in my *2004-2005 Annual Report*, this action in 2005 put our province and Quebec out of line with other Canadian jurisdictions and continued us, until quite recently, on a divergent path away from the more patient-centric, consent based system endorsed by eight other provinces.

In any privacy regime, one could think of the regime as a car engine with six cylinders. For the engine to perform optimally, it requires each of the cylinders firing and in sequence.

In any privacy regime, one could think of the regime as a car engine with six cylinders. For the engine to perform optimally, it requires each of the cylinders firing and in sequence.

In any privacy regime, one could think of the regime as a car engine with six cylinders. For the engine to perform optimally, it requires each of the cylinders firing and in sequence. The six cylinders in our HIPA engine include:

1. The statute itself – HIPA and the Regulations;

2. The government agency responsible for administration of the statute and the leadership for HIPA implementation and administration including the Minister of Health, Deputy Minister of Health, eHealth Saskatchewan Chief Executive Officer, Chief Executive Officers of the regional health authorities, Registrars and Presidents of the regulatory colleges;

3. The Privacy Officer or HIPA Coordinator who provides operational leadership in each trustee organization including regional health authorities, the Saskatchewan Cancer Agency and the regulatory colleges for each of the 27 health professions;

4. The policies and procedures both for those who must comply and apply HIPA and transparency of those instruments for the public so patients can understand what will happen to their most sensitive personal health information;

5. The role and work of the independent oversight agency – the OIPC; and

6. Civil society and the Saskatchewan public.

I will address each sequentially.

1. HIPA and the Regulations

HIPA, unlike the stand-alone health information laws in Ontario, Newfoundland and Labrador and New Brunswick, is not likely to be designated as substantially similar to the federal *Personal Information Protection and Electronic Documents Act* by Industry Canada. This is due to the reliance on sharing of patient personal health information without patient consent in HIPA. Although it was described as a consent-based statute when first enacted, that is only because of section 27 of HIPA and the provision for something described as - "deemed consent". Deemed consent is a confusing expression which, in the HIPA context, means no consent.

To be substantially similar to the *Personal Information Protection and Electronic Documents Act*, the Ontario *Personal Health Information Protection Act, 2004*, adopted the model of "implied consent" for most health information transactions. This brought Ontario's *Personal Health Information Protection Act, 2004* into alignment with the *Personal Information Protection and Electronic Documents Act* and led to the designation of substantially similar by Industry Canada. The effect is that Ontario's *Personal Health Information Protection Act* effectively displaces the *Personal Information Protection and Electronic Documents Act* in that province. Subsequent health privacy laws in Newfoundland and New Brunswick were modelled on Ontario's *Personal Health Information Protection Act* and these have also been designated by Industry Canada as substantially similar to the *Personal Information Protection and Electronic Documents Act*. I might add that the earlier laws in Manitoba and Alberta have suffered the same fate as Saskatchewan's HIPA since they also rely on a no consent model rather than implied consent.

What is the impact of HIPA not being designated as substantially similar? It turns out there is not much prejudice. Although, theoretically Saskatchewan trustees who are operating a private business, such as a pharmacy or a medical clinic, are subject to two different privacy laws at the same time (one federal - the *Personal Information Protection and Electronic Documents Act* and one provincial - HIPA) in practice, the focus is on the health specific HIPA. The federal Privacy Commissioner has the power under the *Personal Information Protection and Electronic Documents Act* to defer a privacy investigation if the matter can "more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of... a province." [section 12(1)(b) of the *Personal Information Protection and Electronic Documents Act*]. Our experience is that this is the approach taken by the federal Privacy Commissioner's office to complaints about Saskatchewan trustees.

... notwithstanding the lack of patient-first features in HIPA, the privacy standard for the electronic health record being constructed by eHealth Saskatchewan is much higher than no consent.

A further consideration is that, notwithstanding the lack of patient-first features in HIPA, the privacy standard for the electronic health record being constructed by eHealth Saskatchewan is much higher than no consent. This will be discussed below in the section dealing with that Crown corporation.

There are legislative changes that my office has been recommending for a number of years. Key amendments proposed by our office were outlined in my *2011-2012 Annual Report* (page 38) and included:

- Allow the OIPC to share information with Information and Privacy Commissioners in other jurisdictions where necessary to undertake a joint or at least coordinated investigation where more than one jurisdiction's health information law is engaged. We find more cases where personal health information moves over provincial borders and an investigation into a related privacy breach requires collaboration with the oversight office in a different jurisdiction. This also has been recommended by the Canada Health Infoway Health Information Privacy group.

- There are serious limitations in the definition of "trustee" such that a number of persons or organizations that have custody of personal health information cannot be held accountable under HIPA for what they do or fail to do with that personal health information.

- There is a need to ensure that HIPA also applies to volunteers, contractors, physicians with hospital privileges and ensure parallel obligations and duties for those persons.

- Revisit the provision for deemed consent to bring HIPA into closer alignment with the reality of the electronic health record under construction in Saskatchewan.

- Revisit sections 8 and 18.1 of HIPA which were designed for a different electronic health record model than the distributed database system now being constructed As presently worded, Saskatchewan patients may never actually have the right that those sections purport to confer on patients. This is because the six elements of section 18.1 of HIPA contemplate a large single database and not the distributed network which is being built.

There has, however, been no action by the Government of Saskatchewan to address those issues. In my *2009-2010 Annual Report* on page 19, I discussed the need for a permanent solution to the problem of abandoned patient paper records which continues to bedevil the regulatory colleges and our oversight office. This is an issue our office identified as early as 2008 and it is disappointing that no permanent solution has been achieved over the intervening five years.

A significant problem has been how to ensure compliance by trustees with HIPA. As discussed in my *2009-2010 Annual Report,* I have been concerned with the lack of serious consequences for employees of a trustee that snoop in patient personal health information for purposes other than diagnosis, treatment or care of that particular patient. There are two kinds of safeguards for ensuring compliance. There are 'soft' safeguards such as:

... I have been concerned with the lack of serious consequences for employees of a trustee that snoop in patient personal health information for purposes other than diagnosis, treatment or care of that particular patient.

- Education of trustee employees;
- An oath or pledge of compliance with HIPA requirements;
- Policy and procedures in the organization for HIPA compliance;
- Cautions or prompts when entering an electronic database;
- A sign-in requirement to identify the purpose of viewing someone's personal health information; and
- An audit capacity of the electronic health records and an ongoing proactive audit program.

There are two major 'hard' safeguards:

- Dismissal from employment of a trustee for cause; and
- Prosecution under section 64 of HIPA.

In Saskatchewan we have had a number of cases where it appears that the 'soft' safeguards have been insufficient. They have not been effective in deterring trustee employees from snooping in the personal health information of a patient(s). Yet neither of the two 'hard' safeguards appear to be available to trustee organizations. When employees responsible for health records in regional health authorities have abused their access to health records by snooping for their personal reasons and have been terminated by their regional health authority employer, terminations in at least some cases have been overturned on arbitration. In each case, a modest penalty of a number of days without pay was substituted.

Yet on the other hand, the threat of prosecution seems also ineffectual. There is an offence provision in section 64 of HIPA with major penalties of up to $50,000 for an individual and $500,000 for an organization. In my Investigation Report H-2011-001, I recommended that the Minister of Justice, whose permission is a condition precedent to any prosecution, consider a prosecution for a breach that resulted in some 180,000 pieces of personal health information of patients being discovered in a large recycling bin in south Regina. Approximately one year after my report and recommendations were issued, the Minister announced that there would be no prosecution. He did indicate that there would be a high level consultation involving the Ministries of Health, Justice and other organizations that would consider alternatives including amendment of HIPA or perhaps some form of administrative penalties. Our office has not been invited to participate in this consultation and we are not aware of any report resulting from this study group.

In my Investigation Report H-2011-001, I recommended that the Minister of Justice, whose permission is a condition precedent to any prosecution, consider a prosecution for a breach that resulted in some 180,000 pieces of personal health information of patients being discovered in a large recycling bin in south Regina.

As it stands, we cannot be sanguine that if an employee of a trustee organization snoops that there will be an appropriately serious response. We think this must be apparent to everyone in the Saskatchewan health sector as well. What is disheartening is that in other Canadian provinces, a zero-tolerance approach has resulted in prosecution in a number of cases that include Ontario, Newfoundland, British Columbia and Alberta. We have seen that large fines following convictions in Alberta have had a salutary impact on compliance by custodians in that jurisdiction. This province appears to be out of step with these other provinces which have a stand-alone health information law. I discussed this issue in the context of a particular privacy investigation in my Investigation Report H-2013-001.

In the meantime, it becomes critically important that all trustees consider how they can strengthen the soft safeguards and enhance the effectiveness of their training, policies and procedures. This may require specifically addressing the impacts of breaching HIPA. In my Investigation Report H-2013-001, I offered a number of recommendations with respect to ensuring that the purpose for which someone

snoops in personal health information is irrelevant if it is not for a professional treatment purpose. I have recommended that a zero tolerance approach be implemented throughout the province. This does not mean that dismissal for cause should follow every breach. It does mean that, if an employee deliberately snoops in a trustee organization that has appropriate policies and procedures and has provided appropriate staff training, dismissal for cause should apply unless there are special extenuating circumstances – in other words dismissal for cause should be the default punishment.

There has been a need for regulations since HIPA was first proclaimed in 2003. In 2004, the Ministry of Health published a set of proposed regulations. Our office participated in the public discussion and submitted a formal response dated September 10, 2004 entitled *Report on The Health Information Protection Act Draft Regulations* which is available on our website – www.oipc.sk.ca. Unfortunately, since 2004, areas that could benefit from regulations have not been addressed at all. This includes fees for patients exercising their right of access and record disposition schedules and rules.

I note that section 63 of HIPA contemplates regulations to address some 25 different matters, yet the only regulations in place as of March 31, 2013 relate to disclosure to law enforcement authorities, to the Department of Learning and disclosure of personal health information for fundraising purposes, as well as a listing of "designated archives".

With respect to the fundraising regulations, we expressed at the time a number of concerns about that regulation since it permitted the disclosure of some personal health information to foundations for fundraising purposes without the prior express consent of patients. Notwithstanding the regulation, we are encouraged by the decision of all regional health authorities to continue to require express consent before there is any such disclosure for fundraising purposes.

Notwithstanding the regulation, we are encouraged by the decision of all regional health authorities to continue to require express consent before there is any such disclosure for fundraising purposes.

Of great concern to our office is that we only recently learned that some regional health authorities have determined that allowing their staff to enter electronic databases to view their own personal health information is encouraged as a means of identifying errors in that information. This is a dangerous and worrisome practice that we think sends the wrong message to staff. It confuses the right of a patient to enjoy access to their own personal health information and the "use" transaction that happens when a health worker views the personal health information of any patient in the electronic information systems of their trustee organization. To be an appropriate use, the staff person would need to be viewing their own information for purposes of

diagnosis, treatment or care or direct support of such activities. It is unethical, however, for a provider to diagnose or treat themselves when in a health care facility. It also deprives the regional health authority of the opportunity to meet its requirements as a trustee under section 38 of HIPA to consider if there is, in the record, personal health information of third parties, information the release of which may compromise someone's health or safety or information that relates to a quality of care investigation or perhaps even a criminal investigation.

In addition to those concerns and perhaps most important, once you allow health staff the ability to enter electronic databases for purposes entirely unrelated to diagnosis, treatment and care, you send a confusing signal that it may be acceptable to snoop in the personal health information of a family member, a neighbour, a former spouse, a business rival or some prominent person in the community.

2. Ministry of Health and Leadership

Although the privacy team working on the electronic health record for a number of years was, for a time, part of the Ministry of Health when it was known as the Health Information Solutions Centre, it was subsequently moved to the newly created Crown corporation – eHealth Saskatchewan. My plan is to deal with the electronic health records not in this section but in the section entitled *eHealth Saskatchewan*. That will, however, also reflect work done by the Ministry of Health before the creation of eHealth Saskatchewan in late 2011.

The Ministry of Health has assisted the 13 regional health authorities in the development of policies and procedures for HIPA implementation originally and compliance now. It has a number of resources on its website related to privacy, HIPA and the electronic health record.

The Ministry of Health was responsible for the development of HIPA, the implementation of HIPA in September 2003 and since that time has had the administrative responsibility for HIPA.

The Ministry of Health has assisted the 13 regional health authorities in the development of policies and procedures for HIPA implementation originally and compliance now. It has a number of resources on its website related to privacy, HIPA and the electronic health record. A good example is the six panel brochure entitled *The Health Information Protection Act (HIPA)*. This brochure is both accurate and informative. It has undertaken a number of training sessions for trustees and it responds to requests for assistance and advice from trustee organizations. Through the Network of Inter-Professional Regulatory Organizations (NIRO), it supports the work of the health profession colleges and regulatory bodies in their HIPA compliance efforts. Although later in this section I will identify concerns with the quality and

appropriateness of a number of the policies and procedures that have been developed for regional health authorities, I want to acknowledge that, at this time, it appears that the regional health authorities do, for the most part, have policies and procedures to govern the collection, use and disclosure of, access to and correction of personal health information. This work has been facilitated and coordinated by the Ministry of Health. The Ministry of Health has participated in the planning of the Prairie Health Information Privacy Day conferences organized by my office, the Manitoba Ombudsman, Office of the Information and Privacy Commissioner of Alberta and Office of the Information and Privacy Commissioner for British Columbia and its successor - the Western Canada Health Information Privacy Symposium. It has also participated in the annual Access, Privacy, Security and Record Management Forum organized by the Access and Privacy Branch, Ministry of Justice. In addition, the Ministry of Health has been a key participant in the planning of a Privacy and Security Month awareness program. For each of the last three years this has been a pan-government activity.

The Canadian experience with health information laws is that the best way to avoid or minimize privacy breaches is to do a better job at the front end of each health care transaction. At different times over the approximate ten years of HIPA, we have observed the Ministry of Health devoting a good deal of time and energy to trying to collect data on all breaches, attempting to coordinate breach responses of all regional health authorities, and directing trustees on how to respond to specific breaches. This appears to have been at the expense of development of tools, resources and training to assist those same trustees to achieve full and robust compliance with the many requirements of HIPA. My respectful suggestion is that Saskatchewan patients would be better served if the Ministry of Health would, as quickly as possible, provide all trustees and the public with a comprehensive and detailed manual and more training opportunities for HIPA compliance.

Compared with what is available on the Ministry of Health website in Manitoba, Alberta and Ontario about their stand-alone health information statutes, there is not a great deal of useful and accurate material for patients on the Ministry of Health website. If one clicks on "Health Information Protection Act (HIPA)", that leads the viewer to 12 documents as well as the statute itself and the regulations. Some of the documents are intended for trustees and others for patients. Some of this information is outdated. Most of the material ignores both changes in the information management practices of Saskatchewan trustees over the last decade as well as recommendations issued by our office in our oversight capacity. Much of this material on the Ministry of Health website is not written or designed to be easy to follow and readily accessible to the public. What follows are some observations about a sample of these resources on the Ministry of Health website.

i. *The Health Information Protection Act Quick Reference Sheet*

This reference sheet discusses consent but in a confusing and inaccurate fashion. It suggests that there is some meaningful difference between deemed consent and no consent. It appears to have been written before HIPA even came into force and does not account for the changes in the practices and understanding of HIPA that has evolved and changed since 2003. It does not clearly indicate that data minimization and the need-to-know are general duties not limited to the deemed consent provisions in section 27 of HIPA.

ii. *An Overview of the Health Information Protection Act*

This document is dated August 2003. It claims that "The Act is consistent with international standards for managing personal health information..." HIPA cannot even qualify as being substantially similar to the federal *Personal Information Protection and Electronic Documents Act* because of its treatment of consent, including the peculiar deemed consent feature. Our province's failure to meet those international standards was again apparent in 2005 when only this province and Quebec refused to sign the *Pan Canadian Health Information Privacy and Confidentiality Framework* because apparently it did not want to move to the higher standard of implied or express consent. Saskatchewan, in this respect, has been very much acting in a way that is inconsistent with national and international standards. To be fair, notwithstanding that HIPA and the Ministry of Health's original interpretation of it was pointing our province away from the national and international standards, the work of eHealth Saskatchewan in adopting the higher standard of implied consent for purposes of the electronic health record does align us much more closely with other jurisdictions. The problem now is that the Ministry of Health's public information about HIPA and personal health information generally is at significant variance with the electronic health record being developed by eHealth Saskatchewan. If we ignore what work is being done by eHealth Saskatchewan and focus only on the Ministry of Health, we would need to say that the Ministry of Health's information for the public about the 'comprehensive health record' does not acknowledge that it would be near impossible for all of the elements of the definition to be met and consequently it may never be an option for a patient to exercise a veto over other health care workers viewing their personal health information.

... notwithstanding that HIPA and the Ministry of Health's original interpretation of it was pointing our province away from the national and international standards, the work of eHealth Saskatchewan in adopting the higher standard of implied consent for purposes of the electronic health record does align us much more closely with other jurisdictions.

As I had indicated in my Investigation Report H-2013-001, the discussion about a 'circle of care' is extremely unhelpful and inconsistent with strict application of the

need-to-know rule which is part of HIPA. Yet this is prominently featured in this publication on the Ministry of Health's website. In my office's experience, the utilization of circle of care by the Ministry of Health in its training materials and programs has contributed to an attitude of entitlement of health care workers who believe they are still free to snoop in someone's health record even when they have no legitimate need-to-know. The question about whether trustees can sell or market personal health information does not account for the 2010 fundraising regulations that do allow a regional health authority to disclose some personal health information about individuals to an outside agency for the purpose of fundraising.

iii. *Overview of Consent Requirement in The Health Information Protection Act*

This piece is dated July 2005. This is not helpful since it does not deal with consent for treatment or service, yet that exclusion would capture the vast majority of disclosures of personal health information under HIPA. The title of this document will no doubt be confusing since it suggests it will be comprehensive. There is a disclaimer on page one but this may not be clear and understood by many readers.

iv. *Changes to Health Information Protection Regulations*

This document is about the regulations made in 2010 to allow regional health authorities to disclose some personal health information to other organizations for fundraising purposes. This is not an accurate description of the regulations and contributes to the confusion of what is personal health information by subdividing it into confusing, non-statutory categories. The document inaccurately claims that only names and addresses can be shared, but the enabled disclosure by regional health authorities would also disclose the fact that the subject patient received a health service in a particular health care facility and when.

There is an application form to download from the Ministry of Health website for someone who wishes to make an access request under HIPA. Unfortunately, there is no indication to the patient that this is not a prescribed form and all that is required is that the patient submit a letter requesting access.

There are a number of other resources intended obviously for trustee organizations. There is room for improvement. In fact, updating the materials for the public on the

Ministry of Health website would be an excellent way to mark the 10th anniversary of HIPA's proclamation.

I should also note that one brochure for the public was produced at some point in 2012 but was never shared with our office before it was published. When another trustee brought it to our attention, we found that it included significant errors and at our request it was removed from the Ministry of Health website. That was in the early fall of 2012 and although we have provided considerable input, we understand that the brochure has not yet been satisfactorily revised to accurately reflect HIPA. Unlike other jurisdictions, the Ministry of Health has not pursued opportunities to develop co-branded educational materials for HIPA compliance and to consult with this office on a regular basis to improve the quality of the common policies and procedures.

There has been considerable turnover in staff in the Ministry of Health's Information Policy unit which manages both FOIP and HIPA. Those tasked to work on HIPA are also tasked with a wide range of policy work unrelated to HIPA. These factors tend to inhibit the development of expertise in HIPA specifically and privacy generally.

In addition, our experience is that there appears not to be an adequate internal privacy training program for new employees in the Health Information Policy unit. Perhaps as a direct consequence, there are long delays in the OIPC reviews and investigations that involve the Ministry of Health. This includes unreasonable multi-month delays for us to obtain the responsive record and the necessary submission. On several occasions we have had to escalate matters to the Deputy Minister.

After we found many privacy officers in trustee organizations were unclear about the terms used in HIPA and privacy law more generally, we developed a *Glossary of Common Terms – The Health Information Protection Act (HIPA)*. Regrettably, the Ministry of Health has promoted different terms and definitions. For example, in our breach investigations we discovered that too many health workers saw themselves as members of a circle of care which is a term utilized by the Ministry of Health in its materials and training. Despite our advice that the practical effect of this term was to expand the list of those who believed they were entitled to collect, use or disclose a patients' information far beyond the need-to-know requirement in section 23(1) of HIPA, the Ministry of Health advised that some trustees were familiar and comfortable with the term and that it would continue in the Ministry of Health's lexicon. Their concession was that they would now explain that to be in the circle of care, you must have a need-to-know. The effect of this approach is to make what should be a simple concept, far more complicated than necessary. Our experience is that the more complicated trainers make HIPA, HIPA compliance will suffer.

After we found many privacy officers in trustee organizations were unclear about the terms used in HIPA and privacy law more generally, we developed a *Glossary of Commonly Used Terms – HIPA*.

In considering leadership more generally, in too many cases too little attention is focused on the information rights of patients and what is required to properly address those information rights. I am often told by some Privacy Officers in those larger trustee organizations that their recommendations for improving the management of access requests and privacy investigations are often ignored or rejected. I am mindful that in a health care system that is chronically stressed to deal with the myriad health needs of our population, there may never be sufficient resources to do everything that a regional health authority may wish to do. Nonetheless, ensuring that attention is paid to the information rights of patients is an intrinsic element of a patient-focused health care system. To the extent that this is the stated objective of the Ministry of Health and indeed the Saskatchewan Government, I expect that our regional health authorities overall can do a better job of managing access requests and privacy complaints, and taking proactive action to address privacy and access issues.

I also note that the Ministry of Health apparently mandated Quality of Care Coordinators/Client Service Representatives in each regional health authority even though there is no statutory mandate for such a role yet it has apparently been unable to mandate the appointment of a Privacy Officer with prescribed responsibilities to ensure that HIPA requirements are met on a consistent basis.

Although the College of Physicians and Surgeons and the Saskatchewan Medical Association produced a useful *Privacy Toolkit*, a number of the regulatory colleges initially did not accept that they played a pivotal role in the implementation and administration of HIPA. This view meant little was done by those colleges to assist their members to prepare for the successful implementation of HIPA. The result was no tools or resources, no guidelines, no frequently asked questions, no sample policies, no sample procedures and no sample forms.

Some of the regulatory colleges have suggested to us that their mandate is focused on the enabling statute for their particular profession or discipline and that it didn't include HIPA. Our position is that self-governing health professions are expected to protect the public and that includes ensuring that the information rights of patients are respected and enabled. Partly as a result of the notoriety attached to the data breach, that is described in our Investigation Report H-2011-001, we have observed in the last two years that the regulatory colleges have started taking more proactive steps to build HIPA compliance by their members.

I encourage the Chief Executive Officers of our 13 regional health authorities, and the Saskatchewan Cancer Agency to consider how they can attach more value to the often thankless work of their Privacy Officers.

In discussing leadership on the HIPA files, I must note that on August 10, 2012, the Minister of Justice and Attorney General announced that there would be no prosecution of Dr. Teik Im Ooi, in respect to the mismanagement of a large volume of personal health information discovered in a recycling bin on March 23, 2011. In my Investigation Report H-2011-001, I had recommended that the Minister of Justice consider prosecution under HIPA. The Minister indicated that, in the opinion of the Ministry of Justice and an independent law firm, such a prosecution would not likely result in a prosecution. He further indicated that he was creating a working group involving the Ministry of Justice, the Ministry of Health and stakeholders to consider if legislative change is warranted to be able to address these kind of privacy breaches. We have not seen any work product from this group as of the end of the 2012-2013 fiscal year.

3. Privacy Officers and HIPA Coordinators

No job is more important in an access and privacy regime than that of the operational leader – the Privacy Officer or HIPA Coordinator in each trustee organization.

No job is more important in an access and privacy regime than that of the operational leader – the Privacy Officer or HIPA Coordinator in each trustee organization. This may be a good time to remind trustees that the actual processing of access requests or privacy complaints from individuals normally will consume only a fraction of the time of the Privacy Officer. More time should be spent on developing or contributing to policies and procedures, HIPA orientation for new hires and conducting in-service training for existing employees, providing access and privacy advice to senior leadership, promoting proactive disclosure to reduce the volume of formal access requests and monitoring new developments in access and privacy and new case reports from the OIPC.

The Privacy Officer should be responsible for ensuring that formal PIAs are undertaken for new projects that impact the privacy of patients and/or confidentiality of their personal health information. Those responsibilities and the significance of this work should be reflected in the classification of and remuneration for these positions. These Privacy Officers get good at what they do by doing a lot of this work. Retention of that kind of experience is important in order for a trustee organization to do an excellent job meeting their FOIP, LA FOIP and/or HIPA responsibilities. Our impression is that there is a high turnover rate for Privacy Officers.

In order to reduce the length of time that citizens must wait to have their formal access and privacy requests resolved, we will be looking to set firm deadlines for the trustee to provide our office with the responsive record and its submission on why the record

has been withheld or the privacy complaint not satisfactorily resolved. Vacations and long-term leaves happen in every trustee organization so it is important that plans are made to deal with FOIP, LA FOIP and/or HIPA requests for access and privacy complaints during those times and alternate procedures need to be in place to deal with those matters expeditiously.

If a particular file is not progressing satisfactorily, matters will be escalated internally to me as Commissioner, I will then deal with the head of the trustee organization. We will be working hard to compress the time to move a review file conclusion, either by informal resolution or preparation of a formal report within five months of the time that we commence a review in 80% of such files. We will work towards the same five month period to conclude privacy investigations in 60% of such files.

As we discussed in past Annual Reports, a regional health authority must be cautious in assigning this role to someone who is the Quality of Care Coordinator/Client Service Representative as well. Our experience is that this often results in confusion in dealing with patients. When acting as the Privacy Officer, the job is to receive and respond to access requests promptly and quickly. It does not matter what the reason is for the request and the requester is not obligated to discuss other matters with the Privacy Officer. This appears to be quite different than the approach taken by Quality of Care Coordinators who tend to focus more on the motivation of the requester and see the interaction with a disgruntled patient as an opportunity to avoid lawsuits, complaints to Members of the Legislative Assembly and others.

4. Policy and Procedures

I have described section 16 as the 'spine of the HIPA skeleton' because of its importance and the fact that it effectively connects the general duties and the transaction-specific duties of any trustee as well as all other elements of the statute.

I have described section 16 as the 'spine of the HIPA skeleton' because of its importance and the fact that it effectively connects the general duties and the transaction specific duties of any trustee as well as all other elements of the statute.

It would be hard to exaggerate the importance of the section 16 responsibility to have taken reasonable measures, including technical, administrative and physical measures, to protect the personal health information for all activities covered by HIPA. When we encounter a significant breach of privacy, most often we find that the responsible trustee did not have any such policy or procedures or at least no written policy or procedures.

Some trustees have argued that section 16 of HIPA does not explicitly state such policies and procedures must be in writing but our position has been that a failure to codify policy and procedures fails to meet the reasonableness test in section 16. When there are written policy and procedures, too often what purports to be policy and procedures is little more than a recitation of the statutory provisions. This is insufficient. The policy and procedures need to be written in plain language and be focused on the particular activities for collection, use and disclosure, access to and correction of, personal health information within the particular business activity of that trustee organization. An extremely useful resource is the 2010 *Guidelines for the Protection of Health Information Special Edition (Putting it into Practice: Privacy and Security for Healthcare Providers Implementing Electronic Medical Records*). This is produced by Canada's Health Informatics Association also known as COACH.

We often encounter confusion over the respective roles of HIPA and professional codes of ethics. It appears that health profession regulatory bodies can do more in terms of reinforcing the primacy of HIPA. HIPA does incorporate, by reference, professional codes of ethics in several sections but otherwise, HIPA is clearly paramount. For a trustee who has breached HIPA to argue that he or she was acting in accordance with their code of ethics, is not a credible excuse for the breach. Nonetheless, this is a common defence raised by trustees in our breach investigations. Although I discussed this issue in my *2006-2007 Annual Report* (page 11) it became an issue in my Investigation Report H-2010-001 and again in my Investigation Report H-2011-001.

The Saskatchewan College of Physicians and Surgeons provided a *Privacy Toolkit* on its website for its members and a similar resource appeared on the website of the Saskatchewan Medical Association, shortly after HIPA came into force. In investigating breaches however, we have certainly encountered a number of physicians who had done virtually nothing to account for HIPA, and their responsibilities under that Act. I should note that the Saskatchewan Medical Association and eHealth Saskatchewan have collaborated to ensure that when physicians install an electronic medical record system there is HIPA training provided.

... the Saskatchewan College of Pharmacists has embarked on an ambitious mandatory training program for all Saskatchewan pharmacists. This also is a very welcome development.

I am very encouraged by amendments to *The Medical Profession Act* that are currently before the Assembly. These will confer new powers on the College to address a failure by physicians to meet their responsibility for safekeeping their patients' personal health information (both current and former). I applaud this initiative.

In addition, the Saskatchewan College of Pharmacists has embarked on an ambitious mandatory training program for all Saskatchewan pharmacists. This also is a very welcome development.

I should note that a good deal more needs to be done by trustees generally to meet the obligation for prospective transparency in section 9 of HIPA. This provides that:

> Right to be informed
> **9**(1) An individual has the right to be informed about the anticipated uses and disclosures of the individual's personal health information.
>
> (2) When a trustee is collecting personal health information from the subject individual, the trustee must take reasonable steps to inform the individual of the anticipated use and disclosure of the information by the trustee.
>
> (3) A trustee must establish policies and procedures to promote knowledge and awareness of the rights extended to individuals by this Act, including the right to request access to their personal health information and to request amendment of that personal health information.

Although we have not had the resources to regularly audit this at the point of service, and physically survey trustee offices and clinics, our first hand experience to date is that most trustees have failed to address this. Some trustee offices will display a general privacy poster from the Canadian Medical Association, but this makes no mention of HIPA, doesn't identify how to go about making an access request or a breach of privacy complaint, does not mention their right to have a notation made on the record should the trustee refuse a request for a correction, or of the right to appeal to our office and contact information for our office for that purpose. There is little value in affirming the information rights of patients if they are not provided with the necessary information about what those rights consist of and how to invoke them.

We have discovered that the focus by the Ministry of Health on promoting province wide uniformity in policies **and** procedures has also had some negative consequences. First, our concern as an oversight agency is that policies should reflect HIPA requirements and should be similar. Procedures, however, need to account for business practices in any given regional health authority and need to accommodate differences in capacity, sophistication, nature of the community and health care facilities, degree of specialization and critical mass. Our experience is that we have found resourceful and creative health care workers have often devised systems that accomplish the objectives of HIPA but perhaps in ways that may differ from procedures in different regional health authorities.

The other problem is that we have seen time and again, the isolation of the Chief Information Officer Forum's Security and Privacy sub-committee and failure to involve

our office on an ongoing basis in the development of policies and procedures. This has meant mistakes have been compounded by other regional health authorities copying an inadequate or improper policy or procedure in another region; best examples would be those documented in our *Report on Management of Access Requests from patients to Saskatchewan Regional Health Authorities* (December 14, 2009) and *Report on Systemic Issues with Faxing Personal Health Information* (November 23, 2010). Each of those reports discuss policies, forms and processes that were not congruent with HIPA requirements and privacy best practices but which were copied by many other regional health authorities nonetheless.

5. OIPC Role and Works

When I commenced as Saskatchewan's first full-time Information and Privacy Commissioner *pro tem* in November 2003, it was apparent that in the absence of any kind of HIPA manual or sample policies or procedures for trustees, our enforcement oversight work would need to be deferred to an extent in order to provide education and training to familiarize trustees, and employees of trustees, with their new obligations.

The OIPC has delivered some 1,045 educational presentations in more than 34 Saskatchewan communities and most them have addressed HIPA to a greater or lesser extent.

The OIPC has delivered some 1,045 educational presentations in more than 34 Saskatchewan communities and most them have addressed HIPA to a greater or lesser extent. In addition, we prepared more than 29 different resources to assist trustees all available on our website www.oipc.sk.ca.

These included:

- *Report on The Health Information Protection Act (HIPA) Draft Regulations*
- *Privacy Impact Assessment*
- *Helpful Tips: Privacy Breach Guidelines*
- *Helpful Tips: Best Practices – Mobile Device Security*
- *Helpful Tips: Privacy Considerations – Faxing Personal Information and Personal Health Information*
- *Your Privacy and Access to Information Rights in Saskatchewan*
- *A Contractor's Guide to Access and Privacy in Saskatchewan*
- *How to Survive as a FOIP/HIPA Coordinator*
- *Severing Made Easy*
- *Fees, Estimates and Wavers*
- *Duty to Search and Assist*

- *Report on The Health Information Protection Amendment Regulations, 2010*
- Response to discussion paper: *Better Information for Improved Health – A Vision for Health System Use of Information in Canada*
- *Advisory for Saskatchewan Health Trustees for Record Disposition*
- *Report on the Systemic Issues with Faxing Personal Health Information*
- *Advisory for Saskatchewan Physicians and Patients Regarding Out-Sourcing Storage of Patient Records*
- *Report on Management of Access Requests from patients to Saskatchewan Regional Health Authorities*
- *The Promise of Personal Health Records* (Resolution of OIPC and Canada's Privacy Commissioners and Privacy Enforcement Officials)
- Presentation to the Standing Committee on Intergovernmental Affairs and Infrastructure regarding Bill 20, *The Gunshot and Stab Wounds Mandatory Reporting Act*
- Commentary on Bill 6, *The Youth Drug Detoxification and Stabilization Amendment Act*
- Commentary on Bill 20, *The Gunshot and Stab Wounds Mandatory Reporting Act*
- Presentation to Saskatchewan Institute of Applied Science and Technology/ University of Regina Nursing Program, Health Informatics Course,
- Presentation to Saskatchewan Medical Association - Retention/Disposition of Patient Records – HIPA Obligations
- Presentation to Network of Inter-Professional Regulatory Organizations
- Presentation to Canadian Bar Association, Mid-Winter Conference - *Welcome to the Brave New World of Electronic Health Records*
- Presentation to Prince Albert Parkland Health Region Case Management Accreditation Team
- Presentation to Prairie Health Information Privacy Day 2007 - *Access Requests vs. Disclosure*
- Presentation on *The Health Information Protection Act - A Primer*
- Presentation on the *Privacy Laws and Health Information: Making it Work!*

When we issue formal access review reports or privacy investigation reports, we view these as potential training materials and make them very detailed to achieve that end. In total our office has issued six reports that considered denial of access to patients and nine reports that considered breaches of privacy. We opened 253 HIPA case files and closed 236 of them since HIPA was proclaimed.

When we issue formal access review reports or privacy investigation reports, we view these as potential training materials and make them very detailed to achieve that end.

In my *2011-2012 Annual Report* (page 41-42), I discussed four myths that we often confront in our HIPA compliance work and explained why they are inaccurate and serve only to impede sound HIPA compliant practices.

Given the problems we were encountering with patient files being improperly stored or destroyed, we collaborated with the National Association for Information Destruction to organize a workshop in Regina on October 16, 2012. The purpose was to provide trustee organizations in Saskatchewan with the tools for developing data disposal policies and training programs as required by HIPA. This included a CD of electronic templates and forms to assist in policy development and a turn-key information destruction training program and DVD.

6. The Public and Civil Society

Citizens and patients should be able to find, on the Ministry of Health website, a good deal of practical, accurate information about how to make an access request, how to request a privacy investigation, how to request a correction of errors in their medical record, as well as a list and description of the rights conferred on patients and the limitations imposed on trustees by HIPA. There should also be an explanation of their right to appeal to the OIPC if they are dissatisfied with the response they get from the trustee organization in question.

We have encountered a good deal of confusion with respect to section 11 of HIPA and what it means for the collection of the Saskatchewan health services number or any demand by a non-trustee to produce the health services number. We have learned that the health services number continues to be routinely collected by retailers, financial institutions and law firms. We suggested to the Ministry of Health approximately five years ago that our respective offices co-brand an explanatory brochure to assist organizations understand and comply with that provision. No such commitment has been forthcoming from the Ministry. In the meantime, we have communicated with the federal officials responsible for the Financial Transactions and Reports Analysis Centre of Canada compliance regime our concern with over collection of the health services number with the result that changes were made to instructional material issued by the Financial Transactions and Reports Analysis Centre of Canada's office. We have also had discussions with the Law Society of Saskatchewan with respect to the purpose and meaning of section 11 of HIPA. The common problem is that although a government institution or private corporation may have a policy that the health services number or card is not a requirement but may nonetheless be volunteered for identification purposes, staff interacting with the public at the point of service may demand or appear to be demanding the health services number or card in order to obtain a non-health service. This issue was discussed in my Investigation Report F-2012-001 available on our website, www.oipc.sk.ca.

There is a need for a simple brochure explaining the rights of the patient with respect to their personal health information uploaded to the electronic health record. I might add that Canada's Health Informatics Association has produced some excellent materials that could be useful in designing information materials for patients.

In my *2005-2006 Annual Report* (page 26), I raised questions about the quality and appropriateness of the materials developed by the Chief Information Officer Forum's Security and Privacy sub-committee. I stated that:

> In my *2003-2004 Annual Report* I drew attention to the concern that Saskatchewan Health had not committed adequate resources to the implementation of HIPA. That concern remains. That concern is compounded by staff turn-over and the demands on the department from the increasing use of PIAs by Saskatchewan Health itself and a variety of projects managed by the department. It may be a product of inadequate resources, but a number of the educational materials produced by Saskatchewan Health tend to be 'high-level' or overviews. These materials are not perhaps as helpful as they could be for staff working in trustee organizations and requiring a comfortable understanding of what they can and cannot do in light of HIPA. This office has and will continue to provide input in the development of further tools for trustees. In my advice to trustees I have recommended a focus on very practical, concrete information to assist trustees. This could involve specimen forms, decision-trees, checklists, diagrams to simplify the process of assessing whether a particular collection, use or disclosure is appropriate and assessing requests for access or correction and other practical tools.

I have similar concerns with the material that exists for public awareness.

Given the fact that electronic health records will involve everyone who lives in Saskatchewan and a major challenge with electronic health records is ensuring strong public confidence, my suggestion is that a good deal more time and effort should be devoted to dialogue with the public about the electronic health record.

In a number of Canadian provinces, civil society groups have vigorously participated in debate and discussion with respect to new privacy laws including stand-alone health information statutes such as HIPA. This has not, however, been the experience in this province. It does not appear that Saskatchewan has seen significant activity by civil society groups with respect to information rights (both access to information and privacy) and that is unfortunate. I say this since key decisions about the architecture and the operating rules for the electronic health record are made without strong public input.

In a number of Canadian provinces, civil society groups have vigorously participated in debate and discussion with respect to new privacy laws including stand-alone health information statutes such as HIPA.

Health professions and their organizations have been intensely involved in the electronic health record initiative given their projected prominent role as users of the electronic health record. The Ministry of Health, as has been the case with other provincial health ministries, has identified significant efficiencies and is heavily invested in the development of electronic health records. In fact, the Deputy Minister of Health is on the Board of Directors of Canada Health Infoway, the federal-provincial-territorial non-profit corporation, that is coordinating the Pan-Canadian interoperable Electronic Health Record system.

Regional health authorities are also active participants in the electronic health record development. My observation is that when all of these groups come to the table to discuss and determine how the electronic health record will operate, the empty chair and the unheard voice is that of the rest of us who will receive the health services – the patients.

This is where privacy comes into play since privacy is uniquely the right of the individual to exercise a measure of control over his or her personal information. There have been some belated efforts to redress this oversight. This includes the welcome creation by Canada Health Infoway of the Privacy Forum with a representative from each provincial and territorial health ministry and a representative from each privacy oversight body. Canada Health Infoway also requires that a PIA be done on all Canada Health Infoway funded projects and submitted to the privacy oversight body in order to qualify for Canada Health Infoway funding for projects built in Saskatchewan.

In my Investigation Report H-2010-001 I dealt with a pharmacist who abused his role as a user of the Pharmaceutical Information Program to view the drug profiles of persons who were not his patients. In a Postscript appended to that Report I observed as follows:

> The development of an EHR requires a complex balancing of a number of competing goals or values. Obviously the success of any iEHR initiative will require the cooperation and full participation by Saskatchewan health care professionals. There are many examples of features of the iEHR plan in Saskatchewan designed to address the convenience of those professionals. It is also true that while privacy of Saskatchewan residents is important it is not an absolute right and from time to time may be limited to accommodate certain legal requirements, safety requirements and public policy imperatives. The challenge is to find a way of balancing those values which may from time to time be in conflict. In my view, the evident preoccupation with making the iEHR simpler for health care professionals – the providers - has to a large degree eclipsed the need to make our iEHR

sufficiently respectful of the expectations and rights of the patient. This preoccupation with accommodating the preferences as well as the needs of providers perhaps accounts for some of the vulnerabilities exposed in this investigation. Fortunately, our iEHR is still a work in progress. There is still the opportunity to recalibrate – to implement stronger controls and safeguards to better protect the interests of the patient. I think such action is consistent with the thrust and recommendations of Commissioner Dagnone in his *Patient First Review Report* and specifically the following observation:

> Fundamental to achieving patient- and family-centred care is patient-centred governance and policy-setting, beginning with the Ministry of Health and supported by unified, prudently managed, high-performing health care administration that enables, empowers and expects everyone to put the patient first.

Given that we have not seen the engagement of civil society groups on the electronic health record, I suggest it is important that there be more opportunity for Saskatchewan residents to learn a good deal more about both the benefits and the risks associated with the electronic health record.

Western Canada Health Information Privacy Symposium

A number of our regional health authorities and trustee organizations were represented at this health information conference in Calgary on April 30 - May 1, 2012. This conference was organized by the Information and Privacy Commissioners of British Columbia, Alberta, and Saskatchewan and the Manitoba Ombudsman. This proved to be a good opportunity to compare and contrast the experiences in these four western provinces with the electronic health record systems they are currently developing.

This has been an annual event that grew out of a Prairie Health Information Privacy Day conference organized by our office in Regina in 2007 that focused on comparing the experience in the three prairie provinces with Canada's first three stand-alone health information laws. The Ministry of Health has been represented on the steering committee for each of these annual conferences and usually has provided speakers for this event.

eHealth Saskatchewan

eHealth Saskatchewan has generally done a good job in addressing the statutory requirements of HIPA.

eHealth Saskatchewan has generally done a good job in addressing the statutory requirements of HIPA.

We have identified concerns, however, with respect to certain key features of the early domain repositories of the Saskatchewan electronic health record system. A number of these were discussed at length in my *2007-2008 Annual Report*, pages 20 to 26 and my *Annual Reports* 2009-2010, 2010-2011 and 2011-2012 and also a presentation entitled *Welcome to the Brave New World of Electronic Health Records* on our website.

These include such questions as:

- Who will be accountable to the patient for what is done with their personal health information?
- Will patients have a genuine right to opt-out of the electronic health record?
- Is the designed global masking feature at the domain level of various repositories an adequate measure to allow patients a reasonable level of control over their personal health information?
- Why doesn't our Saskatchewan electronic health record allow masking closer to the point of service and why can it not be selective masking rather than global masking?
- Is the list of circumstances which allow for unmasking or 'breaking the glass' of masked personal health information reasonable and in line with patient expectations?

Also, in our *2007-2008 Annual Report* we urged the Health Information Solutions Centre of the Ministry of Health to consider "how patient portals can be facilitated for Saskatchewan residents as an integral element of the move to electronic medical records and EHRs." We have been following with interest developments with patient portals in the University Health Network in Toronto and the patient portal being developed by the Alberta Department of Health and Wellness. We understand that eHealth Saskatchewan is considering making something similar an earlier deliverable than what was contemplated just a few years ago.

eHealth Saskatchewan advises that in the past fiscal year the following PIAs and PIA Supplements were completed:

- Electronic Health Record/Saskatchewan Laboratory Results Repository Release 6.0 PIA Supplement;
- Primary Health Care – Saskatchewan Laboratory Results Repository Integration PIA Supplement;
- Pharmaceutical Information Program Phase 3.1 PIA Supplement;
- Provider Coverage Viewer; and
- Radiology Information System/Picture Archiving and Communications System Stage #4 (Phase 2).

In each case, our office was provided a copy of the PIA and the opportunity to provide extensive feedback on each.

Issues we have raised after reviewing the detailed PIAs include:

- The PIAs indicate that systems like Saskatchewan Laboratory Results Repository and Radiology Information System/Picture Archiving and Communications System rely on a mixed consent model, but mostly rely on deemed consent from section 27(2) of HIPA. The PIAs do not demonstrate that express or implied consent have been carefully considered before the decision to rely on deemed consent. As we have noted in our publications, deemed consent which is in effect no consent, is the approach that is hardest to reconcile with a patient-first approach which has been declared as a high priority for the Government of Saskatchewan and the Ministry of Health.

- A lack of proactive auditing is evident. PIAs indicate that a proactive auditing feature should be implemented but the PIAs offer no timelines or plans. We have recently been advised that eHealth Saskatchewan has commenced a process to install the FairWarning audit system.

- From what we have seen, there appears to be a lack of procedure in place to revoke, suspend, or terminate user privileges in a timely fashion.

The following PIAs and PIA Supplements are underway:

- Panorama Detailed PIA;
- Electronic Medical Record Program Detailed PIA;

- Chronic Disease Management – Quality Improvement Program High Level PIA;
- EHR/Saskatchewan Laboratory Results Repository Release 7.0 PIA Supplement;
- Mental Health and Addictions High Level PIA;
- Person Health Registration System PIA Supplement;
- Provincial Renal Data System PIA;
- SendOuts (Human Resources recruiting system) PIA; and
- Vital Statistics Transfer Detailed PIA.

The PIA process and forms are currently the subject of the Privacy and Access Unit's LEAN initiative. We understand that the plan is to streamline the process and forms so PIAs can be completed in a more efficient manner.

eHealth Saskatchewan also operates a privacy service (eHPS) that:

- Currently supports the Pharmaceutical Information Program, Picture Archiving and Communications System and the eHR Viewer;
- Answers questions or concerns the public may have – the public can contact the service directly by calling a toll-free number or sending an email;
- Deals with requests for audit reports to show who has viewed personal health information;
- Deals with requests to mask personal health information; and
- Deals with requests to remove the mask on personal health information.

I am particularly impressed with the work now underway to allow patients to request a full block in eHR Viewer. The expectation is that this full block feature will be available by the end of June 2013.

I am particularly impressed with the work now underway to allow patients to request a full block in eHR Viewer. The expectation is that this full block feature will be available by the end of June 2013. I have in the past stated that patients should have the right to decide with their primary provider to keep certain prejudicial information outside of the electronic health record. I have therefore considered that selective masking at or close to the point of service would be optimal. eHealth Saskatchewan has indicated that, at this time, it will not include that feature. Given that decision, the next best thing would be a full block in the eHR Viewer. eHealth Saskatchewan intends to allow the patient to unblock their personal health information although their personal health information becomes available to all other registered users unless and until the patient chooses to restore the full block. This appears to achieve what was contemplated by sections 8 and 18 of HIPA.

The important feature of the full block is that unlike the regular masking option, the block cannot be lifted without the express consent of the patient.

Another important service provided by eHealth Saskatchewan is the Privacy and Access Unit's audit and monitoring support, including:

- Creating audit reports upon request by a trustee in order to assist in privacy investigations and complaints; and
- Creating audit reports upon request by an individual to see who has viewed their personal health information in Pharmaceutical Information Program, Picture Archiving and Communications System, and the eHR Viewer.

As I previously stated, I am advised that eHealth Saskatchewan is currently in the process of implementing the FairWarning audit and monitoring software. Initially this will support the Pharmaceutical Information Program and the eHR Viewer auditing. Next steps include monitoring services to the regional health authorities and the Saskatchewan Cancer Agency.

I am also advised that in 2012-2013 the eHealth Privacy and Access Unit within eHealth Saskatchewan has implemented a privacy and security information incident management policy and process. As a consequence,

- All reported information incidents are triaged and investigated; and
- The eHealth Saskatchewan Privacy and Access Unit has enhanced tools to assist its customers in their investigations of incidents.

I encourage eHealth Saskatchewan to make available to the public, on at least an annual basis, statistics on reported "information incidents".

I have concerns with how this province will achieve full and appropriate accountability to the patient for everything done with the patients' personal health information. This concern is due to the proliferation of registered users of our expanding electronic health record system and the shared service models which focus on multi-trustee committees making decisions about collection, use and disclosure of personal health information.

Secondary Purposes for Use and Disclosure

In this last fiscal year, we reviewed a new initiative from the Canadian Institute for Health Information entitled: *Better Information for Improved Health – A Vision for Health System Use of Information in Canada*. This contemplated making more use of

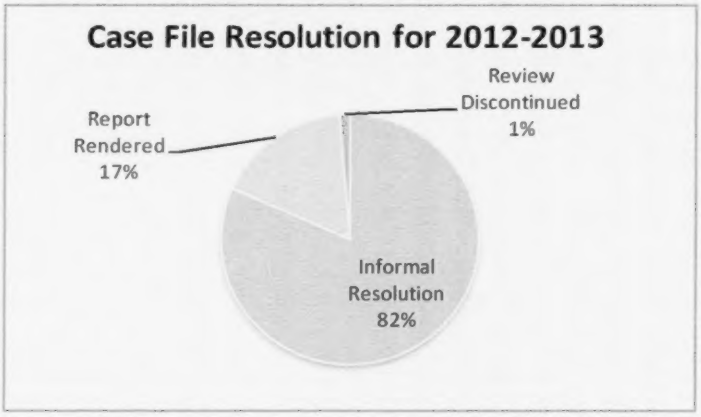
the personal health information collected from patients for purposes of diagnosis, treatment and care, for purposes not directly related to that provision of service to the patient. It was not at all clear that this would occur only after the individual had provided express consent to such secondary sharing of their personal health information.

The traditional understanding has been that if a health care organization wishes to make use of the patient information for any secondary purpose, they would need to disclose this to the patient first and obtain their consent. One of my concerns is that, before creating new uses for identifiable personal health information, our health system needs to demonstrate that it is satisfactorily protecting the privacy of patients and the confidentiality of their personal health information. We have not yet reached that point. My office's submission can be viewed at www.oipc.sk.ca under the *What's New* tab.

The Freedom of Information and Protection of Privacy Act

Addressing the Backlog

The 2012-2013 fiscal year has been remarkable for the number of old files closed by the OIPC and the record number of formal reports issued. This office has been bedeviled for many years by too many case files which then became a big backlog as we simply did not have the capacity to move the large volume of files to completion. Completion would be either by way of informal resolution or by the issuance of a formal report and, in rare cases, by discontinuance of a review.



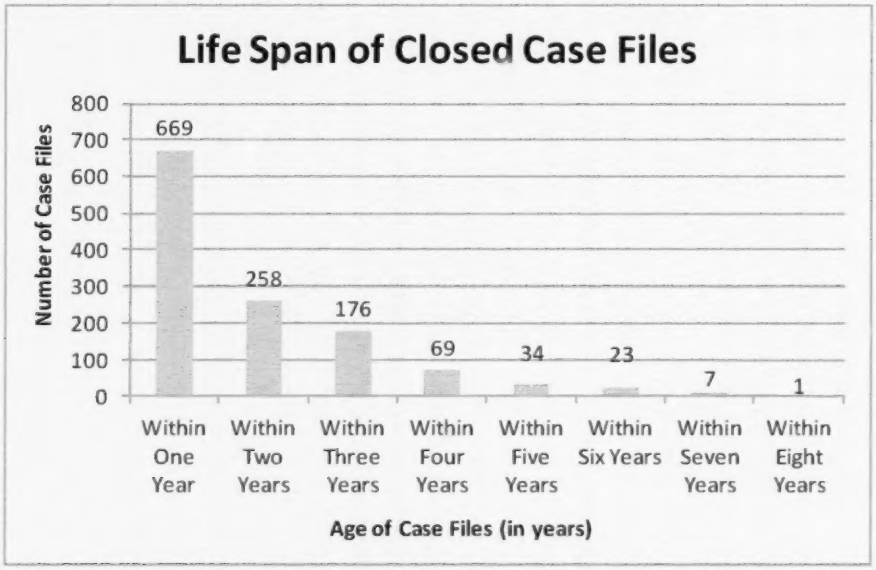
At the heart of the backlog were many files that were matters of first impression for our office, files that involved large volumes of records, or files on which we could not get timely cooperation from the public bodies in getting the responsive record and/or getting a written submission in support of the exemptions claimed.

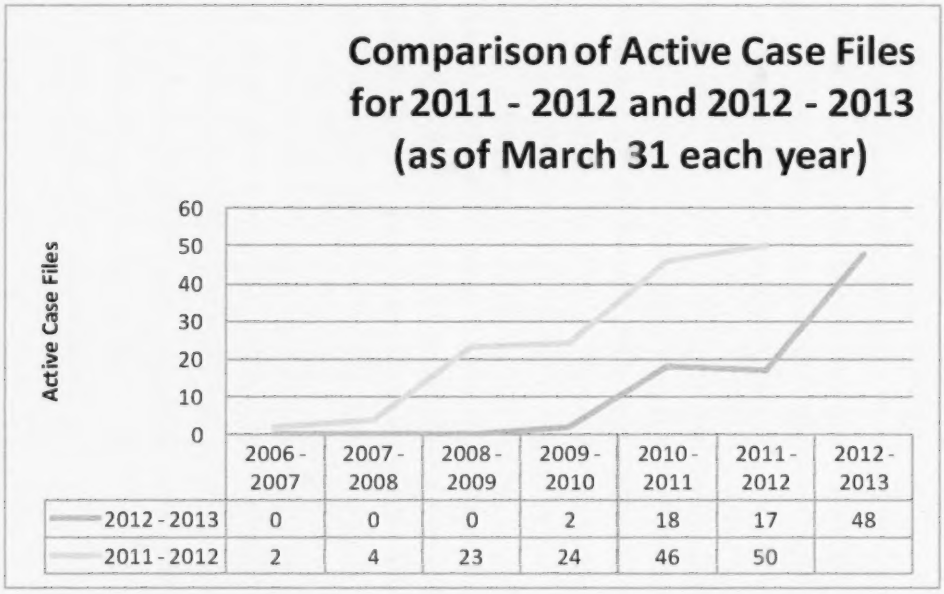
A further complication has been unfamiliarity with FOIP even in some of our largest Ministries, and attempts to introduce new exemptions many months or often many years after the Ministry provided its formal response to an applicant and indicated why it was denying access.

As a result of a great deal of internal planning led by our Director of Compliance and our Director of Operations and some internal reorganization plus the coordinated efforts of three skilled and productive Portfolio Officers, we were able to close 147 case files. We were also able to produce 16 case reports now available on our website: www.oipc.sk.ca. Most importantly, we have managed to close all case files older than 2009-2010 but for two. We have closed 28 files opened in 2010/2011 and 17 files

... we were able to close 147 case files. We were also able to produce 16 case reports now available on our website: www.oipc.sk.ca.

opened in 2011/2012. At this rate by the end of 2013-2014, we should have no file older than two years and few that are more than a year old. Our long term goal of closing 80% of our reviews of access denial within five months and 60% of privacy investigations within five months may still be out of reach unless we have more Portfolio Officers but it is certainly becoming much closer.





I should caution that the statistics noted above capture reviews and investigations under all three of the statues we oversee, although the largest number of files relate to reviews of access denied under FOIP. Appendix 1 is a breakdown of those public bodies involved in requests for reviews released in 2012-2013. Appendix 2 is a breakdown the public bodies involved in requests for reviews concluded in 2012-2013.

The Role of the Ministry of Justice

As noted earlier in the context of assessing progress with HIPA compliance, I discussed the need to consider not just the legislation but also the role and work of the actors in the access and privacy regime. In the case of FOIP, the other major actor is the Ministry of Justice. It is this Ministry that is tasked with administrative responsibility for FOIP. This responsibility entails providing tools and resources to the public bodies in Saskatchewan to promote compliance with FOIP and collecting statistics and tracking performance of public sector bodies. A good description of the mandate of the Access and Privacy Branch, Ministry of Justice can be found in the *2011-2012 Annual Report of the Ministry of Justice and Attorney General*:

It is this Ministry that is tasked with administrative responsibility for FOIP. This responsibility entails providing tools and resources to the public bodies in Saskatchewan to promote compliance with FOIP and collecting statistics and tracking performance of public sector bodies.

> The Access and Privacy Branch **provides internal access to information and privacy services for the Ministry** and provides leadership and advice on access and privacy issues to Government and local authorities, works with and provides support to access and privacy officials across the Government to help with specific issues, develops training programs, and assists with education of public sector employees. [emphasis added]

This description of the mandate of the Access and Privacy Branch, Ministry of Justice is similar to the description in earlier years save for one significant addition that is underlined in the quote above. The addition is the provision of access and privacy services for the Ministry of Justice itself. This means that, as the Ministry of Justice starts to receive more access requests and privacy complaints, more of the resources in this small office of four permanent full-time employees must be devoted to processing those matters, at the expense of the training and support to access and privacy obligations pan-government and of local authorities. I expressed concern about this development in the Postscript to my Review Report F-2012-006.

The Access and Privacy Branch, Ministry of Justice organized another successful Privacy and Security Awareness Month in May 2012 and also a major conference in

The Access and Privacy Branch also delivered training sessions, and hosted regular Access and Privacy Forums for FOIP Coordinators to improve knowledge of the law and consistency of practice.

Regina in June 2012. Both of these were excellent initiatives that build on work done by the Access and Privacy Branch in earlier years. The Access and Privacy Branch also delivered training sessions, and hosted regular Access and Privacy Forums for FOIP Coordinators to improve knowledge of the law and consistency of practice. The Access and Privacy Branch also responds to requests for assistance from government institutions, local authorities and the public to help with understanding and compliance with access and privacy requirements. The Ministry of Justice also held a LEAN event to identify possible improvements in the processing of access requests received by government institutions.

I note that according to the statistics in the *2011-2012 Annual Report* from the Access and Privacy Branch, Ministry of Justice:

- There has been an increase from 43% to 48% where access to general information was granted in full.
- Access has been fully denied in only 5% of requests for general information whereas the average of the four previous fiscal years was 10%.
- There has been an increase from 27% to 35% where access to personal information was granted in full.
- There has been a decrease of approximately 10% in requests for personal information that were fully denied.

These statistics show encouraging progress in promoting transparency.

As noted in my Postscript to Review Report F-2012-006, that Ministry also serves as the legal advisor to many of the same public bodies when they seek advice about FOIP or wish to deny an access request and they may even represent the public body when our office undertakes a formal review under Part VII of FOIP.

In our experience, the Ministry of Justice, presumably on the instructions of their respective clients, is raising new discretionary exemptions months, and in some cases years, after the review has started, and takes an excessively narrow and legalistic view of the 'right of access to information' and a very broad view of the mandatory and discretionary exemptions to that right.

The Ministry of Justice has adopted interpretations of "personal information" and "third party" that result from not considering both FOIP and LA FOIP as complementary pieces of an access and privacy regime but rather by ignoring the other statute. Information that would not qualify as "personal information" under FOIP is treated by the Ministry of Justice as "personal information" for purposes of LA FOIP and vice versa. Although nationally, "third parties" would not include a public body, according to our Ministry of Justice a local authority can be a third party under

FOIP and a government institution can be a third party under LA FOIP. These interpretations lead to, what I suggest would be, an absurd result. These interpretations cause confusion for both the public and public bodies given the clear direction of our Court of Appeal and the purpose of both laws. These issues are explored in my Review Reports F-2012-006 and F-2012-003.

In my opinion, the Ministry of Justice, in doing its work as legal advisor to many public bodies, appears from time to time to lose sight of its other role which is to promote transparency and accountability of public bodies and protecting the privacy of citizens and to ensure that public sector employees are trained accordingly.

It is for that reason, I have suggested that the Government of Saskatchewan consider moving the Access and Privacy Branch out of the Ministry of Justice and away from its adversarial role in contesting the right to know on individual files and instead relocate the Access and Privacy Branch to a different Ministry such as the Ministry of Central Services that has a different kind of service focus. Such a Ministry would presumably be better placed to promote access and privacy rights of citizens without an adversarial agenda.

There are other reasons why I am suggesting that the Assembly consider such a structural change. In the event that I recommend prosecution under the offence provisions of section 68 of FOIP, section 56 of LA FOIP or section 64 of HIPA, no such prosecution can occur without the express consent of the Attorney General. Yet in many cases, it is the agents of that same Attorney General who have been providing advice and counsel to the public body throughout the processing of an access request or investigation of a privacy complaint.

While I have no doubt that the Attorney General and his agents will act appropriately and professionally in assessing a possible prosecution, the relationship may create public doubt that the decision to prosecute or not will be assessed independently and fairly. Interestingly, neither Alberta nor British Columbia require the consent of the Attorney General to initiate a prosecution under their access and privacy laws.

The Canadian experience over the last 30 years is that to create a culture of openness and privacy protection requires a lot of work and focused, effective leadership. We are speaking of transitioning from a regime where the information held by government belongs to government and is only disclosed when government chooses to do so, to a culture where citizens have rights to information not dependent on the generosity of their government. Our office's experience is that the Ministry of Justice has not demonstrated that it is the most appropriate ministry to lead this cultural shift. In addition to concerns already identified in this Annual Report, materials produced by the Ministry of Justice reinforce my view.

If one examines the Ministry of Justice *Plan for 2013-2014* there is very little focus on either access or privacy in the 28 page plan. Before the Access and Privacy Branch, Ministry of Justice was created approximately five years ago, the *2004-2005 Annual Report* produced by the Ministry extensively reviewed a very long list of priorities, activities and achievements but made no mention of its role in administering FOIP or LA FOIP in the entire 56 page document. This seems odd given that the Ministry of Justice had FOIP responsibility since 1992. In fact the word "privacy" appears but a single time but that was in the context of victims' services and likely relates to concerns raised by the Privacy Commissioner of Canada with the Royal Canadian Mounted Police. The organization chart at page 41 does not even identify FOIP or LA FOIP as a specific responsibility. It is hard not to conclude that, in a Ministry with a very broad mandate and a very long list of statutes for which it has responsibility, FOIP and LA FOIP seems to get lost or at least is close to the bottom of the Ministry of Justice's priorities.

A key action in the *Plan for 2013-2014* discussed in some detail relates to the Hub and the Centre of Responsibility broad strategy in Prince Albert to build a safer community. There is no acknowledgement that this strategy involves the collection, use and disclosure of personal information and personal health information and that only recently has there been a decision to make some changes in the way the programs operate after my office made inquiries in late 2011 about compliance with FOIP, LA FOIP and HIPA.

I note that in the *2004-2005 Annual Report* for the Ministry of Justice there is a reference to a Central Steering Committee formed by the Ministry of Justice and the Ministry of Corrections and Public Safety. The described purpose was to oversee the targeted initiatives such as the Prince Albert intersectoral working group considering "new and innovative ways to meet the needs of at risk youth...". No reference is made to the need to ensure this strategy, in all of its dimensions, conforms to the applicable law or the need to make further changes. Yet, I would suggest that such a review and remedial action should have been a high priority for the Ministry of Justice given the prominence of this project and the proliferation of similar groups in other Saskatchewan communities.

The same *Plan for 2013-2014* has a strategy to promote a favourable business environment and better protect consumers by improving legislation but there is no plan apparently to consider adopting a private sector privacy law such as the law in British Columbia and Alberta that has many advantages over the federal law that currently applies to most Saskatchewan businesses. Unlike the current situation in Saskatchewan, the British Columbia and Alberta model applies to trade unions, non-profit organizations and to virtually all employee information in the private sector.

The *Plan for 2013-2014* acknowledges "increased requests for information under *The Freedom of Information and Protection of Privacy Act*". Yet, the Ministry of Justice's response to date has been to task the Access and Privacy Branch, which has a mandate to promote awareness and training throughout government, with responsibility to assist in processing individual access requests to the Ministry of Justice. This likely means that the comprehensive FOIP manual, that is urgently required in our province, will be further delayed and that important training work will be postponed.

There is another key action that is to: "Continue to develop and implement consistent records management policies and procedures to enable retention security and disposition of records in accordance with legislative obligations and other business interests." In addition, there are key actions related to the privacy of all clients in public registries. Yet, surely both of these key actions miss the most obvious and most serious gap in FOIP and that is no obligation for each government institution to protect the personal information in its possession or control including requiring administrative, technical and physical safeguards. There is also no offence provision for failing to take reasonable measures to protect personal information and consequentially, no penalty for such an offence. The most impactful and significant way to ensure the appropriate retention, security and disposition of records is to address this legislative gap, a gap that is unique to Saskatchewan among Canadian provinces and territories.

In its *2011-2012 Annual Report of the Ministry of Justice and Attorney General*, it is noted that: "Proposed amendments to *The Securities Amendment Act, 2011* were introduced in the Fall 2011 Legislative Session. The Act is intended to support the work of the Canadian Public Accountability Board and authorizes the SFSC [Saskatchewan Financial Services Commission] to regulate credit rating organizations." The Report goes on to discuss the Ministry of Justice's work with respect to the same Bill. The Ministry of Justice, according to its *2013-2014 Business Plan* is providing legislative policy advice to the Financial and Consumer Affairs Authority (FCAA) of Saskatchewan "including participation in federal/provincial/territorial working groups." Yet when Bill 65 - *The Securities Amendment Act, 2012* received first reading in the Assembly, it provided in part that certain records notwithstanding FOIP must be held "in confidence". To do so, the Financial Services Commission must be of the opinion that: "(a) the person to whom or **company to which the information in the record relates would be unduly prejudiced** by disclosure of the information, and the person or **company's privacy interests outweigh the public's interest** with respect to disclosure..." [emphasis added]. The reference to a company having a privacy interest is an obvious error. This error reflects a lack of awareness of the modern concept of privacy. Fundamental to the

legal concept of privacy is that a corporation has no privacy interest and no right of privacy.

Privacy, as understood for many years and as articulated by the Supreme Court of Canada on numerous occasions is a concept and an interest uniquely of the individual.

Privacy, as understood for many years and as articulated by the Supreme Court of Canada on numerous occasions, is a concept and an interest uniquely of the individual. A corporation may have a confidentiality interest but this is quite different than the right of privacy and certainly has no constitutional protection in the way that privacy does.

More concerning is that I alerted the Minister of Justice to the error in Bill 65 on March 22, 2013 but, as of the end of the fiscal year, we have received no confirmation that the error will be corrected before the Bill is passed. Although we could find no similar error in the Alberta, British Columbia, Manitoba or Ontario comparable legislation, even if another province(s) should make the same error in the course of the national collaboration, we would hope that our Ministry of Justice would be sufficiently familiar with privacy law to register an objection and not include it in the Saskatchewan Bill.

What is more, nothing in either the Bill nor in the Minister of Justice's comments in *Hansard* suggest that it considered any options to protect confidential information other than the outright exclusion. One would hope that the Ministry responsible for our access and privacy law would first consider less drastic remedies such as reliance on an exclusion or even a paramountcy provision. As we have indicated to the Minister, a number of other provinces do not appear to have gone so far as to create the same kind of broad exclusion from their freedom of information laws.

Another key action in the Ministry of Justice's *Plan for 2013-2014* is: "Through a collaborative process with other ministries and agencies, finalize and communicate the processes and guidelines for sharing information in integrated service initiatives and implement the distribution plan." Given the experience with the Hub and the Centre of Responsibility in Prince Albert, there should be reference to the need for more rigour in any new personal information sharing arrangements to ensure full compliance with FOIP, HIPA and where applicable LA FOIP.

Right to Know Week 2012

The week of September 24 to 28 was officially recognized as Right to Know Week in Saskatchewan by means of proclamations issued by the Government of Saskatchewan and by the Cities of Saskatoon and Regina.

On September 27, 2012 in Saskatoon, Professor Dr. Stephen Maguire from Carleton

University spoke at the College of Law on *Professionalism, Accountability and Transparency in Policing*. The Regina Public Library also organized a public film series during Right to Know Week to highlight the themes of transparency and accountability to citizens. On October 3, 2012 in Regina, Wayne MacDonald, Director of the Government Services Program and the online Information Access and Protection of Privacy (IAPP) Program at the University of Alberta delivered the keynote address. The topic was *Celebrating 20 Years of FOIP Legislation in Saskatchewan.*

The *Chief Justice E.M. Culliton Right to Know* Award was presented to the City of Regina. The award was accepted by City Manager and the Director of Information Services. Since 2006, this award has been presented on an annual basis to public sector bodies that have demonstrated leadership or innovation in promoting the public's right to know.

The City of Regina was selected largely on the basis of its achievement in becoming the first public sector organization in Saskatchewan to adopt an ambitious program of Open Government – Open Data. It was applauded for its actions in making data sets freely available to the public on an open licence basis with more data sets to come in the future. It is also publishing records that were previously released in response to access to information requests. A notable feature of the City of Regina's initiative has been the close collaboration with non-government groups that create new applications for the data that the City of Regina now has released or contemplates releasing.

Past award recipients include the Saskatoon Regional Health Authority, Health Quality Council, Saskatchewan Institute of Applied Science and Technology and the Crown Investment Corporation.

I want to acknowledge the sponsors and our partners: Johnson-Shoyama Graduate School of Public Policy, Institute of Public Administration in Canada (SK), Canadian Bar Association, Regina Public Library, Sheldon Chumir Foundation for Ethics in Leadership, McDougall Gauley LLP, MacPherson Leslie & Tyerman LLP, Gerrand Rath Johnson LLP, University of Saskatchewan, and the University of Regina.

FOIP Coordinators and the 'Good Faith' Defence

From time to time, we encounter FOIP Coordinators who will advise us that they have received advice from a lawyer or some other source that is different than the recommendations that our office provides with respect to the three statutes we oversee. These FOIP Coordinators are concerned about what they should do when

faced with conflicting advice. We encourage those FOIP Coordinators to consider four facts:

1. The OIPC is the only body designated by the Assembly to oversee government institutions, local authorities and trustees under FOIP, LA FOIP or HIPA, other than the Court of Queen's Bench. The Court is only involved if an applicant is dissatisfied with the public body's or trustee's response to recommendations from the OIPC and then takes steps to appeal to the Court. There has, however, been only one such appeal under one of these Acts in the last nine years. In that appeal, the Court adopted the OIPC analysis and findings and converted our recommendations to the Kelsey Trail Regional Health Authority, to release the information to the applicant, into a binding order.

2. Even if a court should at some future date take a different view than the OIPC on interpretation of any of the three statutes, what would be the consequence? It would mean that our office and all public bodies and trustees would need to modify their practices to account for that court decision. It normally wouldn't have retroactive application. Even then, there is a good faith defence available to any FOIP Coordinator who is following the advice of the OIPC. That provision is section 67 of FOIP, section 55 of LA FOIP and section 62 of HIPA. Any FOIP Coordinator that is following the advice of the oversight body (either the OIPC or a Court) should be well protected by reason of the good faith defence even if at some future time, a higher authority should decide something different.

3. The OIPC strives to be consistent in its interpretation of the three laws and is guided by direction from the Saskatchewan Court of Appeal, the Supreme Court of Canada and a very large body of jurisprudence and Commissioners' orders and decisions from Canadian jurisdictions. We strive, wherever our specific legislation allows, to harmonize our approach with the direction of the courts and practices in other provinces.

4. Advice received from other sources is just that – advice. The design of the three statutes is that each government institution, local authority or trustee may consider advice from different sources but must ultimately make the decision and be responsible for that decision.

The Local Authority Freedom of Information and Protection of Privacy Act

In my *2011-2012 Annual Report*, I discussed the need for there to be monitoring of the activities of local authorities under LA FOIP. Currently, the only reporting required is that of the Ministry of Justice that provides statistics in an Annual Report on certain FOIP activities of provincial government institutions. In most other provinces, it is common for the Government to report on both activity of government institutions and also that of local authorities. The Government of Saskatchewan has not given any indication of whether it is prepared to address this gap.

We reiterate our call for FOIP and LA FOIP to be integrated into a single statute which will allow only one set of forms and harmonized rules with respect to fees and exemptions. A single integrated law can also address explicitly the drafting oversight in not accounting for third parties and personal information which appear to be defined differently in FOIP and LA FOIP. I repeat and incorporate herein that commentary from my last Annual Report and many previous Annual Reports.

In my last Annual Report, I identified a concern with respect to how to meet the statutory burden of proof on a review as highlighted in a number of reports involving the City of Saskatoon. I want to acknowledge the excellent cooperation we have seen in this past year from the City Solicitor's office and the City Clerk's office in that city which has led to a more collaborative and productive approach to reviews which involve the City of Saskatoon.

I have been encouraged by a new project undertaken by the Saskatchewan School Boards Association with new funding from the Ministry of Education. This brings together education stakeholders to collaborate on the creation of a kind of LA FOIP on-line handbook for schools and educators. Our office has been consulted on this project and provided clarification as to our interpretation of LA FOIP and our expectations for school divisions in meeting their access and privacy responsibilities. We also continue to encourage school divisions to designate a FOIP Coordinator to ensure heightened attention to orientation and in-service training for school staff and more consistent handling of both access requests and privacy complaints.

We also continue to encourage school divisions to designate a FOIP Coordinator to ensure heightened attention to orientation and in-service training for school staff and more consistent handling of both access requests and privacy complaints.

We encountered an interesting situation under LA FOIP that is related to my Investigation Report LA-2012-002. In the course of our privacy investigation we concluded that it would be a good idea for the regional health authority to implement a privacy enhancing tool, namely to utilize a web robot exclusion protocol. We understood that the regional health authority had considered that recommendation.

Subsequently, we were advised by the Ministry of Health that it believed "the issues of transparency and accountability far outweigh the perceived risks to employees" and therefore it is not prepared to undertake steps to utilize the protocol as "there is no evidence this will prevent the perceived risks noted in your report." My view is that if the regional health authority is prepared to consider this preventative measure to better protect its employees it should be free to do so. In any event, our recommendation was based on expert advice from industry leaders to the effect that the risk to the privacy of the employees in question is a real one and that risk warrants use of privacy enhancing technologies such as the web robot exclusion protocol. It seems odd to argue as the Ministry of Health appears to be doing that in effect there is no point in locking the door to your house since thieves can still break a window and enter your house that way. There is no suggestion that the protocol that we recommended is perfect and will prevent all misuse of that information but it reduces the risk nonetheless. I encourage the Minister of Health to reconsider its role in rejecting recommendations we would make to any regional health authority.

As noted elsewhere in this Annual Report, in this past year we saw the conclusion of the first appeal from one of the laws that we oversee to the Court of Queen's Bench. We were encouraged that the Court accepted our analysis, agreed with our conclusions, findings and recommendations and converted our recommendation into a binding order.

In another LA FOIP report (Review Report LA-2012-004), the Board of Education of the Saskatoon School Division No. 13 took an interesting position in opposing the release of a contract it had with a taxi company. It argued on the OIPC review that if the terms of the contract were released, it might allow a competitor an advantage when it came time to consider a new contract. My view is that if there is more transparency about existing contracts to allow a more competitive bidding process in the future that should be advantageous to taxpayers. I recommended release of the contract but the Division refused to follow that advice.

National Freedom of Information Audit 2012

In the National Freedom of Information Audit 2012 undertaken on behalf of Newspapers Canada top marks went to Nova Scotia, Newfoundland and Saskatchewan for completeness of disclosure. The City of Saskatoon received an A grade for timeliness and an A grade for comprehensiveness. The City of Regina received an A grade for timeliness and a C grade for comprehensiveness. The Government of Saskatchewan fared not quite so well with a B for timeliness and a B for comprehensiveness. Between April and August 2012, the same requests were sent to federal government agencies, five departments in each province and 20 municipalities (including Saskatoon and Regina). The authors of the study caution readers about drawing conclusions about any institution's overall record solely from the results of this audit. "No claim is made that the audit requests filed to any one institution are necessarily representative of the overall performance of the institution in answering all requests it receives and it would be an error to interpret them this way." My office's overall experience with Saskatchewan public bodies is a little less optimistic but all of us can certainly celebrate a lot of achievement by local authorities, government institutions and health trustees over the last six or seven years.

When this survey was first published seven years ago Saskatchewan placed dead last and was awarded an F grade. The latest Audit can be viewed at www.newspaperscanada.ca/public-affairs/FOI2012.

Open Government - Open Data

A major theme in my Annual Reports for 2010-2011 and 2011-2012 was that of Open Government. There have been further developments in the 2012-2013 fiscal year.

A major theme in my Annual Reports for 2010-2011 and 2011-2012 was that of Open Government. There have been further developments in the 2012-2013 fiscal year. The City of Regina has continued to make additional datasets available to the public at no cost. The City has worked effectively to collaborate with hacker organizations to develop new applications and uses for the different types of information now in the exclusive possession of the City. The City of Saskatoon has committed funding to investigate an Open Government model for that municipality.

My office also participated in a well attended Regina conference - Saskatchewan 3.0 Summit on Open Government - Open Data on April 24 and 25, 2012. This included featured presentations by Mr. David Eaves, and Dr. Nicholas Gruen. My presentation on *'Open Government' – A Saskatchewan Perspective* is available on our website: www.oipc.sk.ca under the *Presentations* tab.

I continue to encourage the Government of Saskatchewan to create an Open Government - Open Data regime at the provincial level. Both British Columbia and Alberta have already launched Open Government initiatives. This would enhance transparency of government to citizens and also create exciting opportunities for the private sector and non-profit organizations to develop creative new applications for the data now in the possession of government Ministries. This should be done in conjunction with a review of FOIP, LA FOIP and HIPA by the Assembly.

As part of such an Open Government - Open Data initiative, the province should consider how to make more information available to the public easily and at no cost. That would include the ability of citizens to make online access to information requests. Regrettably, Saskatchewan public bodies still require citizens to go to the trouble of finding the prescribed form, complete it in hard copy and then submit it by mail to the public body.

In our *2010-2011 Annual Report* we encouraged the Government of Saskatchewan to allow online requests for records and online responses similar to the process in the United Kingdom, Mexico, and other nations with more modern legislation.

Case Report Summaries

Review Report LA-2012-002

(Kelsey Trail Regional Health Authority)

Summary

Review Report LA-2012-002, issued on April 26, 2012, involved the Kelsey Trail Regional Health Authority (KTRHA). At issue was the refusal to provide the Applicant with the names of registered nurses on duty at the Melfort Hospital on a certain date. KTRHA withheld all of the responsive record citing sections 20 and 23(1) of LA FOIP as justification to deny access. I determined that the employee numbers of the nurses qualified as personal information under section 23(1)(d) and should be severed from the pages. The remaining information in the pages did not qualify as personal information under section 23(1). I also determined that KTRHA failed to meet the burden of proof in establishing the applicability of section 20 of LA FOIP (disclosure could threaten the safety or the physical or mental health of an individual). In particular KTRHA failed to establish any link between certain complaints from the Applicant about physiotherapy treatments he received and a threat to the safety or health of nurses working a particular shift a year prior to the issues relating to the physiotherapy. I was also not persuaded by claims by KTRHA that the fact the Applicant made complaints to the Quality of Care Coordinator, his Member of the Legislative Assembly, the Chairperson of the KTRHA, the Saskatchewan Ombudsman and others was in some way abusive or evidence of a threat to the safety of the staff. Further I found that KTRHA did not accurately represent certain court proceedings that involved the Applicant. I held that the threshold to deny access is not a low one. That threshold cannot be achieved on the basis of unfounded, unsubstantiated allegations. I found that the foundation for the KTRHA decision to deny access was woefully weak. There appeared to have been a total lack of rigour in the assessment of the alleged threat. I therefore recommended release of the remaining portions of the records at issue.

Recommendations and Response

On May 25, 2012, my office received KTRHA's response to the recommendations I made in the above noted Report. KTRHA advised that it would not comply with my recommendation to release the information in question and provided no response to

my second recommendation regarding the need to protect the identity of future applicants from those not involved in processing access applications.

The Applicant then initiated a *de novo* appeal to the Court of Queen's Bench pursuant to Part VI of LA FOIP. The appeal decision was issued by Mr. Justice Zarzeczny on September 19, 2012. The citation is Gregory Evenson v. Kelsey Trail Regional Health Authority, 2012 SKQB 382. I should note that this is the one and only appeal to the Court of Queen's Bench under FOIP, LA FOIP or HIPA in more than a decade.

Mr. Justice Zarzeczny ordered, "in keeping with the recommendation of the [Information and Privacy] Commissioner which I accept and adopt namely..." that the records revealing the identity of the nurses who worked the shift in question be provided by KTRHA to the applicant. In his reasons, Mr. Justice Zarzeczny stated that:

> [8] I have thorough reviewed and considered the Commissioner's lengthy, detailed and comprehensive Report including the analysis of the facts, circumstances, the Act and the law which it contains.
>
> [9] The facts, circumstances, analysis and conclusions which the Commissioner reached in his Report are the same as those that I have reached in my review of this matter *de novo*. I am in complete agreement with the Commissioner's Report.
>
> [10] I have concluded, as the Commissioner did, that the exemption claimed by KTRHA based upon s. 20 of the Act is not established, as it is KTRHA's onus to do. The concerns raised by KTRHA, as most recently reflected in [the KTRHA CEO]'s letter dated May 23, 2012, do not have any basis or foundation in fact. Nor are they supported by any circumstances which are established in the materials that were presented to the Commissioner and that are now presented for review upon this appeal to this Court. The analysis of the Commissioner on this important point is conclusive as against the KTRHA. I conclude, as did the Commissioner, that the exemption contained in s. 20 has not been established and it does not apply.

Review Report F-2012-004

(Executive Council)

Summary

This Review Report was issued June 12, 2012. Subsequent to the November 2007 provincial general election, the Applicant sought copies of briefing books provided to Ministers of 19 different government institutions. All access requests were transferred to Executive Council for processing. Executive Council denied access to all records relying on section 17(1)(a) of FOIP.

After a preliminary analysis from the OIPC was provided suggesting this exemption would not be upheld, Executive Council invoked a new exemption, section 16(1)(d) of FOIP four years after the review commenced. After advising Executive Council that the burden of proof had not been met for section 16(1)(d) and our intention was to issue a formal report, Executive Council then invoked yet a third exemption, section 16(1). I found that the responsive record included considerable statistical and background information to orient new Ministers that would not disclose the nature of Cabinet discussions nor would it disclose advice given or received by Cabinet ministers. Much of this information would be publicly available quite apart from FOIP. My estimate was that perhaps 70% of the briefing material would clearly not qualify as advice for purposes of section 17(1)(a) of FOIP. Executive Council argued that the briefing notes were unique and required special consideration in the application of FOIP. I was not persuaded that the briefing books constitute "unique circumstances" and that FOIP should be applied differently to them. I noted that some other jurisdictions have amended their access and privacy laws to explicitly treat briefing books and materials in a special way but that is not the case in Saskatchewan. I reviewed the general approach that should be taken in dealing with a record subject to a claim of Cabinet confidence. This included a review of the *Report of the Ontario Royal Commission on Freedom of Information and Individual Privacy of 1980* and the Culliton Report in Saskatchewan. I chose to follow the direction of the Nova Scotia Court of Appeal in O'Connor v. Nova Scotia (Priorities and Planning Secretariat), 2001 NSCA 132. In the result, I found that it would be necessary for any public body asserting a claim of Cabinet privilege to have undertaken a line by line review of the record. It would not be appropriate to simply treat the estimated 10,000 pages as an indivisible whole. To do so would be inconsistent with FOIP. I outlined the six considerations that I would utilize in approaching a claim for exemption by Executive Council. I observed that if Executive Council had undertaken the process of severing contemplated by section 8 of

FOIP, it would have been able to protect all Cabinet confidences and yet make available to the applicant a large body of statistical information and background material that clearly does not qualify as Cabinet confidences. I determined that Executive Council failed to meet the burden of proof to justify any of the three exemptions invoked for all of the material but acknowledged it appeared there was material that would be caught by section 16(1) of FOIP. I recommended that the briefing books be disclosed to the Applicant after severing personal information and the information that properly qualified as "Cabinet confidence" material.

Recommendations and Response

My office was advised on July 9, 2012 that Justice would "go through the records and sever from them information which is not subject to the mandatory exemptions under section 16(1) of FOIP for cabinet confidences, or under section 29(1) of FOIP for personal information". Though I found that the exemption did not apply, Executive Council noted the following: "[w]hile we doubt there will be any need, discretionary exemptions under 17(1)(a) may also be applied." Lastly in its response letter, Executive Council advised that it would be charging the Applicant copying charges "in the range of $1,750.00."

In response to this particular issue, I sent a letter dated August 15, 2012 to Executive Council. I drew to its attention clause 7(2)(a) of FOIP that requires the head to give written notice to the applicant within 30 days after the application is made that the record or portions of it would be made available on payment of the prescribed fee and where or the manner in which access will be made available. I also pointed out subsection 9(1) of FOIP that states an applicant that is given notice pursuant to the aforementioned clause is entitled to "obtain access to the record on payment of the prescribed fee." Section 7 appears to be the only mechanism available to a government institution to apply fees to access to information requests. Further, I noted that requesting fees at this stage would be unreasonable some 54 months after it provided its section 7 response to the Applicant. Though my office's role in this review process is now functus, I urged Executive Council to reconsider the application of fees in this instance.

Executive Council responded by way of letter dated September 6, 2012 advising us that it would not reconsider as "by requiring the applicant to pay for copying costs for the product it receives we believe we are striking an appropriate balance to address the issue, and by doing so, assessing a reasonable fee."

Review Report LA-2013-002

(City of Regina)

Summary

This Review Report was issued February 28, 2013. The Applicant made two requests under LA FOIP for access to records in the possession of the City of Regina that potentially contained third party business information. The City provided notification to the Third Party under section 33(1) of LA FOIP and invited the Third Party to provide its consent to release the records or arguments to support withholding the records in question. The Third Party did not provide its consent but instead argued that section 18(1)(b) and 18(1)(c) of LA FOIP applied to the records and they should therefore be withheld. Despite section 18(1), the City concluded that release of the records was in the public interest pursuant to section 18(3) and advised the Third Party and the Applicant of its intention to release the records. The Third Party proceeded to submit a request for review to my office of the decision of the City in regards to both access requests. The Applicant also requested a review of the same as the City withheld other portions of the record under section 28(1) of LA FOIP. I found that neither sections 18(1)(b) or 18(1)(c) applied to the records in question for both access requests. I also found that section 28(1) did not apply to any of the information severed by the City with respect to the first access request.

Recommendations and Response

I recommended the City release everything withheld in full or in part for both access requests to the Applicant. The City of Regina provided its response by way of letter dated March 7, 2013 stating that it had decided to release the records as recommended. It, however, noted that the records would not be released until the 30 day appeal period had ended in the event the Third Party intends to appeal the decision to the Court of Queen's Bench.

Review Report F-2012-006

(Ministry of Justice)

Summary

This Review Report was issued on December 27, 2012. The Applicant made an access to information request to the Ministry of Justice requesting information pertaining to himself. Justice withheld in full or in part 75 pages pursuant to sections 13(1)(a), 15 (1)(k), 22(b) and 29(1) of FOIP. Justice also applied HIPA denying the Applicant access to his own personal health information but not until December 2012 when the review was all but concluded. I found that Justice had not met the burden of proof in applying section 13(1)(a) and 29(1) of FOIP. Further, I found that Justice had not appropriately applied section 15(1)(k) to the records in question.

Recommendations and Response

I recommended that:

- Justice review its records management practices with regards to prosecutorial records to ensure it is compliant with *The Archives Act, 2004* of Saskatchewan;
- Justice continue to withhold the records in respect to which solicitor-client privilege properly applies;
- Justice should release those records withheld under section 13(1)(a);
- Justice should release those records withheld as the personal information of third parties except for the Victim Impact Statement;
- Justice should provide the applicant with his personal information that had been withheld; and
- Justice should revisit the issue of control insofar as it might apply to records that are in the possession of the Royal Canadian Mounted Police for purpose of prosecution under the Criminal Code of Canada.

Given the numerous problems identified in this report with the role and action of the Ministry of Justice and in light of the fact it is this very Ministry that has had

administrative responsibility for FOIP since 1992, I decided to append a Postscript to my Review Report F-2012-006. In the Postscript I identified problems in the way that Justice handled this request including:

- Lack of familiarity with FOIP and HIPA;
- Lack of diligence and rigour in the search for responsive records;
- Failure to consider the application of HIPA at the appropriate time;
- Failure to assess the relationship between the Royal Canadian Mounted Police and the Ministry of Justice in a criminal prosecution insofar as FOIP is concerned;
- Inability to assemble the record and properly link exemptions to portions of the record;
- Confusion over exemptions; and
- Suggestions that delay might result in more voluntary release of records when the additional records released voluntarily were copies of records previously provided to the Applicant.

I also listed nine steps that should be taken by the Ministry of Justice and every other government institution to improve its FOIP performance. These steps are as follows:

1. Appoint and support a properly trained FOIP Coordinator with a full job description.
2. Plan for coverage for vacations, long-term leaves and transition periods when there is a change in personnel to ensure continuity in meeting legislated requirements for dealing with access requests and reviews by my office. Too often we encounter a complete breakdown in processing access requests and significant delays in our reviews when a single individual in a large organization leaves for any extended time.
3. Plan for how to manage access and privacy responsibilities when there is a reorganization of ministries to ensure there are no unnecessary delays in managing requests and participating in OIPC reviews.

4. Ensure that the organization has carefully reviewed all of its record holdings and its record/information collection, use and disclosure practices and policies to ensure timely retrieval of information requested as part of a modern records management system.

5. Ensure that the Deputy Minister or an Assistant Deputy Minister is tracking performance of that Ministry in responding to requests and resolving reviews with the OIPC under FOIP, LA FOIP or HIPA.

6. Ensure that the Ministry's published business plan includes objectives for meeting all access and privacy legislated requirements in a timely and fulsome fashion.

7. Require that the FOIP Coordinator or a substitute attends the annual access and privacy conference undertaken by the Access and Privacy Branch, Ministry of Justice.

8. Ensure that the written delegation mandated by section 60 of FOIP (section 50 of LA FOIP) is clear. Much of the delay we experience in reviews can be attributed to an ostensible need to consult with "someone higher" in that organization. If the "head" has delegated all or most of his or her authority to a properly trained FOIP Coordinator there should be no need to require months of additional time to "consult with others".

On January 28, 2013, my office received a response from the Ministry of Justice to the recommendations made in my Report. The Ministry of Justice advised my office that it intended to comply with some of my recommendations, but not all. Instead of specifically stating it would release the information that I found did not constitute personal information under FOIP, Ministry of Justice stated it would only "continue to protect personal information as defined in the Act and as required by subsection 29(1) of the Act." Justice did not comply with my recommendation to release records it withheld under section 13(1)(a) of FOIP. Its response on this particular recommendation was that "the Ministry will continue to withhold records as required to do so by clause 13(1)(a) of the Act."

Review Report LA-2012-004

(Board of Education of the Saskatoon School Division No. 13)

Summary

This Review Report was issued November 28, 2012. The Applicant made an access request to the Board of Education of the Saskatoon School Division No. 13 (the Board) for a contract between the Board and a Taxi Company. The Board released the majority of the contract to the Applicant, but withheld certain portions pursuant to sections 17(1)(d), 17(1)(f), 17(1)(g) and 18(1)(c) of LA FOIP. In respect to section 17 (1)(f) of LA FOIP, I observed that "[t]he Board appeared to be arguing that the Applicant, knowing the current taxi contract, may supply the Board with a better proposal than the current contract. This would not appear to prejudice the economic interest of the Board." I found that the information in question that may lead to a more competitive proposal for a future contract does not constitute an undue benefit or loss to the Taxi Company. I found that in all cases the Board did not meet the burden of proof to demonstrate that the exemptions applied.

Recommendations and Response

I recommended release of the withheld portions of the record.

In terms of the one recommendation that I made regarding this matter, the Board advised me in its letter dated December 17, 2012 received in my office on December 20, 2012 that it would not comply.

Review Report LA-2012-003

(Village of Buena Vista)

Summary

This Review Report issued October 2, 2012 concerned three access to information requests that were made to the Village of Buena Vista (the Village) by the Village Mayor. The Village Administrator did not respond to the requests. The problem in this case was that the Mayor is designated as the "head" with responsibility under LA FOIP.

However, the elected Council and Village Administrator did not agree and did not recognize this designation. I found that the Mayor was the designated head of the local authority. Further, I found that the Village was in contravention of section 7 of LA FOIP.

Recommendations and Response

I recommended that the Village Council and the Village Administrator immediately comply with LA FOIP by recognizing the lawful authority of the Mayor as head. As well, I recommended that the Minister of Justice consider whether an offence has been committed pursuant to section 56(3)(a) of LA FOIP by reason of the unwillingness of the Village Administrator and Council to allow the Mayor to discharge her responsibilities as head.

The Village did not provide a response in contravention of section 45 of LA FOIP. In terms of my recommendation that the Minister of Justice consider whether an offence had been committed, my office did receive notice from the Ministry of Justice on October 18, 2012 that it had referred the matter to Public Prosecutions for their consideration. On December 13, 2012, my office received notice that there would be no prosecution in this case.

Review Report F-2012-005

(Saskatchewan Workers' Compensation Board)

Summary

This August 29, 2012 Report concerned three different Saskatchewan Workers' Compensation Board (WCB) claimants who had submitted access to information requests to WCB pursuant to FOIP in 2008, 2009 and 2010 respectively.

In each case, the Privacy Officer/Corporate Solicitor responded to the access requests by advising that the information sought is not subject to the access provisions of FOIP. The consistent position taken by this office since 2003 has been that section 23 of FOIP is a paramountcy provision and not an exclusion from FOIP. I have taken the view that section 23 is not applicable since although there may appear to be a conflict between sections 171.1 and 171.2 of *The Workers' Compensation Act, 1979* and Parts II and III of FOIP, it is possible to read the provisions together so they are complementary and not

adverse. Since one can comply with *The Workers' Compensation Act, 1979* provisions without violating the FOIP provision for access to information, there is no genuine conflict and FOIP prevails. This view has been outlined in detail in Review Report F-2012-002 and Investigation Reports F-2009-001 and F-2007-001.

Recommendations and Response

I recommended that WCB process each of the three access requests in accordance with FOIP. I also recommended that WCB and the Minister responsible for *The Workers' Compensation Act, 1979* resolve this matter by adopting the outstanding recommendations in the 2006 Committee of Review and ensure that FOIP explicitly guarantees injured workers the same rights to access information that exist for all other Saskatchewan residents when they deal with other government institutions and local authorities.

WCB provided its response to the recommendations in my Report by way of letter dated September 11, 2012. WCB indicated that it would not follow my first two recommendations and noted the following with respect to the third: "[t]he WCB has already made the Minister aware of concerns your office has expressed about the relationship between the WCAct, FOIP and HIPA."

Review Report LA-2013-001

(Regina Qu'Appelle Regional Health Authority)

Summary

This Report was issued January 9, 2013. The Applicant, an employee of the Regina Qu'Appelle Regional Health Authority (RQRHA) made an access to information request to her employer for a number of records pertaining to two harassment investigations involving her. RQRHA denied access pursuant to sections 14(1)(d) and 28(1) of LA FOIP. I found that section 14(1)(d) of LA FOIP only applied to a small portion of the record, and found that certain information contained in the withheld record constituted third party personal information.

Recommendations and Response

Bound by an earlier court decision, I recommended release of all third party personal information to the Applicant. I also recommended that the portions of the record that constituted the personal information of the Applicant and that which qualified as work product be released to her as well. Finally, I recommended that RQRHA withhold the third party personal health information referenced in the record.

RQRHA provided its response to my recommendation on February 8, 2013. It indicated it would comply with my recommendation and release all records with a few notable exceptions.

RQRHA agreed with my findings regarding the application of sections 14(1)(d) of LA FOIP and the need to withhold any third party's personal health information.

RQRHA indicated, however, that it did not agree with my finding that "a physician with privileges working in a facility of a regional health authority is captured by the term 'employee' for purposes of LA FOIP" and instead indicated it would treat that individual as a third party. RQRHA stated it would "release this document in compliance with your recommendation through the third party notification process as set out in the Act." On April 16, 2013, RQRHA copied my office on a letter to the Applicant stating that it was releasing the record in question as the Third Party offered no objection.

Finally, RQRHA advised that it believed that a "very small portion of the withheld documents should be redacted based on section 28(1) as the information is the work history of the employee(s)" and indicated it would not release it.

Investigation Report H-2013-002

(Regina Qu'Appelle Regional Health Authority)

Summary

This February 26, 2013 Investigation Report concerned an own motion investigation concerning the RQRHA. In May 2010, the media alerted my office to 17 addressograph cards found strewn about the ground near two facilities of a document destruction company in Regina, 15 of which were later to be found belonging to the RQRHA. The

addressograph cards were apparently found by a member of the public who contacted the Regina Police Service. This office undertook an investigation on an own motion basis after RQRHA informed the OIPC of details of the breach. Even though the displacement of the addressograph cards was the result of actions by an employee of the document destruction company, I found that RQRHA was responsible for the actions of its Information Management Service Provider. I found that RQRHA had inadequate safeguards in place to ensure the proper destruction of the addressograph cards in question.

Recommendations and Response

I recommended that RQRHA supplement and formalize its written procedure in regards to the disposal of records containing personal health information and that RQRHA conduct regular and ongoing audits of the document destruction company to help prevent a similar future occurrence. Such audits would ensure that any employee of the contractor who is managing the destruction of RQRHA has been sufficient trained to do so in accordance with HIPA requirements and that each employee has signed a written undertaking to follow proper procedures in the destruction of personal health information. I also recommended that RQRHA destroy the 15 addressograph cards within 30 days.

In its letter to my office dated April 18, 2013, RQRHA advised that it would implement all three of my recommendations.

Investigation Report H-2013-001

(Regina Qu'Appelle Regional Health Authority)

Summary

This Investigation Report was issued February 1, 2013. Our office was notified of three separate but similar cases where employees of RQRHA used their employee user privileges to electronic information systems to view and/or modify personal health information without proper authority. We undertook investigations into each incident. I determined that the administrative safeguards that RQRHA had in place were inadequate, including the reliance on the non-statutory concept of circle of care in RQRHA's policies, procedures, and privacy training materials.

Recommendations and Response

I made a number of recommendations including the following:

- RQRHA review and revise its administrative, physical and technical safeguards within 120 days in an effort to prevent similar privacy breaches from occurring in the future.

- RQRHA revise its *Privacy Violations – Recommended Actions for Employees Draft Jan'11* document to merge Levels II and III.

- RQRHA completely eliminate 'circle of care' from all materials, tools and resources and substitute 'need-to-know' as the operative rule.

- RQRHA implement a policy that addresses the issue of employees viewing and modifying their own personal health information within RQRHA information systems in question immediately.

- RQRHA complete a PIA for the Enovation system so that it may identify and address the privacy weaknesses of the system, and consider all possible mitigation strategies for the indefinite period that the system continues in use.

RQRHA provided an initial response by way of letter, dated February 7, 2013, requesting that I reconsider specific portions of my Report. Specifically it stated:

> [y]our comments in sections [19][21][22][23][24] of the report regarding the implementation of the recommendations that arose from the Region's investigation of the privacy breaches give the impression that the Region has not acted.

On or about February 11, 2013, I advised RQRHA as follows: "On the basis of your letter, I am not persuaded that our Investigation Report is factually inaccurate."

On March 4, 2013, RQRHA provided its response to my recommendations. It indicated that it would implement all my recommendations except the second. The reasoning provided for not is that:

> "[t]his document is being used in other Saskatchewan health regions as well as other health regions outside of Saskatchewan. RQHR feels it is important to have a

consistent disciplinary approach throughout the province and further discussion with other health regions is important prior to making changes to this document."

Investigation Report F-2012-005

(Saskatchewan Government Insurance)

Summary

This Investigation Report was issued October 31, 2012. My office received a formal 'breach of privacy' complaint that related to the "use" by Saskatchewan Government Insurance (SGI) of personal information and personal health information of the Complainant under *The Automobile Accident Insurance Act* (AAIA). The Complainant alleged that too many employees at SGI had access to her personal information and personal health information. The Complainant was an employee of SGI and had filed an injury claim following a motor vehicle accident. SGI took the position that the OIPC had no authority to investigate these matters since neither HIPA Parts II, IV and V, nor FOIP applied to the Complainant's personal information and personal health information as it related to Part VIII of AAIA. I considered representations from SGI and, consistent with past Reports issued by the this office, concluded that there is no evidence that the Assembly would have intended to create such a gap in legislated privacy protection and that, in fact, there is no such gap as alleged by SGI.

Recommendations and Response

I recommended however that the Assembly amend the appropriate legislation to clarify the rules that will apply to the personal information collected, used and disclosed by SGI in its activities under the AAIA and the role of the OIPC in overseeing SGI's statutory responsibilities under FOIP and HIPA. I also recommended that SGI provide an apology to the Complainant and enhance its user access policies and procedures.

SGI provided its response to my office on December 20, 2012 by way of letter dated December 18, 2012. Though SGI advised us that it would apologize to the Complainant and will continue to review and update its information handling practices regarding customer claims information, it did not agree with my finding that there was a privacy breach in these circumstances.

Further on the second recommendation, SGI noted that it has developed "a staff claims handling procedure that not only advises staff of what they can expect from SGI as their employer, but will assist the company in ensuring that the data minimization processes in place within the company are addressed more rigorously." The extent to which this will address my recommendation to review and enhance its policies and procedures to ensure compliance with FOIP and HIPA is unclear.

Investigation Report F-2012-004

(Saskatchewan Workers' Compensation Board)

Summary

This Investigation Report was issued October 25, 2012. Our office was notified of four separate incidents where WCB mailed personal information and personal health information to unintended recipients resulting in unauthorized disclosures. We performed a systemic investigation into WCB's mail handling practices. WCB alleged that each incident was the result of human error. I found that lack of clear and effective policies and procedures also contributed to three of the incidents. I also found that WCB did not track or monitor these breaches, nor did it deal with the breaches in a consistent and effective manner.

Recommendations and Response

I made a number of recommendations including one regarding the retrieval of personal information and personal health information that had gone astray.

- As I previously recommended in Investigation Report F-2007-001, WCB should revise all policies and procedures to reflect language used in FOIP and HIPA.

- WCB should adopt the mailing recommendations I made in Investigation Report F-2007-001 for the mailing of any personal information and personal health information.

- WCB should establish a mechanism to return or destroy unsolicited personal information and personal health information at the point of collection.

- WCB employees should be educated on unauthorized collections of personal information and personal health information and what to do in the event of an unsolicited collection.

- All mailing procedure documents should be amalgamated into one document that reflects best practices on mailing all personal information and personal health information.

- The term "claim owner" should be defined in the Release of Information – Claim Files procedure document. Policies and procedures should use specific position titles and not slang or proper names for the sake of clarity and keeping material up-to-date.

- Mailing procedures should include specifics on why documents need to be reviewed, who should review them and what should be looked for during the review.

- WCB should improve the manner in which it tracks, reports and monitors privacy breaches in order to better identify systemic issues.

- WCB should improve the ways it investigates and responds to privacy breaches, including more detailed investigation reports and consistent responses that reflect best practices.

- WCB should ensure that the Privacy Officer has sufficient resources to fulfill the roles outlined at paragraphs [150] and [153].

- WCB should follow best practices when attempting to retrieve personal information and personal health information after unauthorized disclosure such as offering to send a courier to pick up the information and suggesting, as an alternative, that it can be entrusted to my office.

WCB provided its response to the recommendations contained in my Investigation Report by way of letter dated October 30, 2012 received in my office on November 2, 2012. In reviewing WCB's response, it is unclear to the extent that it agrees or does not agree to comply with some of my recommendations. For instance, where the recommendation is that WCB amalgamate into one document all mailing procedure documents, WCB advises it "will review the safeguards built into the mail handling process as soon as possible to eliminate any confusion." However, in others, WCB clearly states it accepts the recommendation and will make improvements. Examples

include with respect to how it tracks, investigates, responds, reports and monitors privacy breaches and along with the need to expand its privacy investigation capacity. WCB also accepted my recommendation regarding retrieving personal information and personal health information. The recommendations that WCB clearly refused to comply with include those noted at [198], [199] and [200]. In terms of [199] and [200] that make specific recommendations regarding unsolicited collection of personal information and personal health information, WCB states that it makes no "distinction between solicited or unsolicited collection" as "is not a relevant factor to WCB in its legislatively mandated responsibilities to administer work injuries."

Investigation Report F-2012-002

(Saskatchewan Workers' Compensation Board)

Summary

This Investigation Report was issued August 29, 2012. The Complainant brought forward concerns regarding a telephone conversation that took place between a WCB employee and a trucking company regarding the Complainant's active claim. I found that the company was a third party. As such, I found that there was an unauthorized disclosure of personal information when WCB employee confirmed that the Complainant had an active claim. I also found that, during this conversation, WCB collected personal information of the Complainant from the Third Party without proper authority to do so from FOIP.

Recommendations and Response

My recommendations were as follows:

- WCB provide an apology to the Complainant for disclosing personal information in one case and for collecting personal information without authority.

- WCB should instruct its employees to use the phrase "I can neither confirm nor deny that this individual has a claim file with WCB" if a third party calls to inquire or offer information about an individual.

- WCB should ensure its employees are instructed on the rules governing the collection of personal information and appropriate treatment of unsolicited personal information from third parties

- WCB should add steps to its Procedure 10.2 Information from Inquiries (PRO 05/2008) that require employees to verify the accuracy of personal information it collects.

In its response dated September 11, 2012, WCB advised that it did not agree with my first recommendation to apologize to the Complainant and that it only agreed in part with the second. Instead of stating it would or would not comply with the last two recommendations, WCB instead stated its "policies and procedures attend to this adequately" and "WCB staff collect information from multiple sources as and when they consider it necessary... Workers have ample opportunity to respond to all the evidence."

Investigation Report F-2012-003

(Saskatchewan Workers' Compensation Board)

Summary

This August 29, 2012 Investigation Report resulted from a complaint that WCB disclosed the personal information of four employees to third parties without consent. I found that in this case, sections 171 to 171.2 of *The Workers' Compensation Act, 1979* were not paramount to the privacy protections in Part IV of FOIP. I also found that the information constituted personal information under section 24(1) of FOIP. I determined that the complaint dealing with the disclosure of four employees' personal information to a third party without the four employees' consent and without other legal authority to do so was well-founded.

Recommendations and Response

I offered a number of recommendations to WCB in respect to the findings:

- WCB follow our *Helpful Tips: Privacy Breach Guidelines* in respect to the personal information of the four employees of the private business which was disclosed to third parties without the four employees' consent.

- WCB provide adequate training to its employees to ensure a better understanding of the privacy obligations imposed by Part IV of FOIP.

- The Minister responsible for WCB take steps to resolve the issue of the applicability of FOIP to WCB records.

My office received WCB's letter dated September 11, 2012 in response to my recommendations on September 12, 2012. Instead of stating clearly it would or would not comply with our recommendations, WCB noted the following in terms of the three above noted recommendations:

- We have taken these tips into consideration in the last review of WCB policies.

- WCB staff have been given training first regarding the WCAct and secondarily other privacy legislation. This training will be done for new staff, and updated if significant changes occur in the various laws and/or WCB policies.

- WCB has already made the Minister aware of concerns your office has expressed about the relationship between the WCAct, FOIP and HIPA.

Investigation Report LA-2012-002

(Regina Qu'Appelle Regional Health Authority)

Summary

This Investigation Report was issued May 9, 2012. A number of complaints were received by my office with respect to the Internet publication of the names and precise salaries of $50,000 or more paid to all employees of the RQRHA commencing in 2005. I determined that the information published on the Internet was not captured by the definition of personal information for purposes of LA FOIP since an exception for the salaries of employees of any local authority applied. I further found that even if it had qualified as "personal information", there was authority for the Internet publication. This authority was explicit for the salary information of "members, officers and senior employees" of the RQRHA. For all other employees the authority was by means of a delegation of authority to the Minister of Health who in turn required such Internet publication by means of the combined effect of *The Regional Health Services Act*, *The Regional Health Services Administration Regulations* and the *Annual Report Content*

Requirements issued by the Ministry of Health. Notwithstanding the existence of legal authority for the Internet publication practice, I determined that:

- there were significant risks to individuals by virtue of the indiscriminate Internet publication of the names and salary information;

- there exist privacy enhancing technologies that may significantly reduce the risk to individual employees, but these have not heretofore been required or employed by regional health authorities, the Ministry of Health or the Information Technology Office; and

- RQRHA, the Ministry of Health and the Information Technology Office should consider utilizing the web robot exclusion protocol and other technologies to make more difficult the misuse of that published information about identifiable individuals.

Recommendations and Response

My office received the RQRHA's response on June 7, 2012. In terms of its response to my recommendations, RQRHA advised us that it would endeavour to meet my recommendations to the extent reasonably possible. In response to my first recommendation, the RQRHA advised us that it will develop a policy regarding posting of employee salaries and third party payments which would serve as notification for employees. It also advised that it was in Phase two of a three phase strategy to improve its website to meet or exceed current industry standards including migrating to a platform that would enable it to adapt to new technologies including a web robot exclusion protocol. In the interim, RQRHA is looking into how to implement on its existing internet platform.

The Ministry of Health also provided a response to our office on May 31, 2012. Health indicated that salary publication and its methodology is consistently applied across all health and "it does not intend to change its process and publication requirements for RHAs." Further, Health stated that if any employee is interested, he or she may review the *Annual Report Contents Requirements 2011-2012*.

In terms of the recommendation regarding utilizing web robot exclusion protocol, Health stated that it believes "the issues of transparency and accountability outweigh the perceived risks to employees" and therefore it is not prepared to undertake steps to utilize as "there is no evidence this will prevent the perceived risks noted in your report."

On the question about legislative authority to make employee salary information a public record, Health relies on sections 42 and 55 of *The Regional Health Services Act* to require RHAs to report according to the *Annual Report Content Requirements 2011-2012*.

Finally, the Ministry of Health indicated it will not be altering its current requirements or the submission format of those requirements from regional health authorities.

Subsequent to the issuance of this Report, we have been verbally advised by the Ministry of Health that notwithstanding our Report, it is somehow of the belief that if a document is saved as a PDF document that the salary information of an RQRHA employee cannot be retrieved by a web crawler doing a search based on the name of the employee. Neither RQRHA, nor the Ministry of Health nor their technical experts could particularize the foundation for such a belief. I might add that in the various instruments relied on by the Ministry of Health to obligate regional health authorities to publish specific salary information of employees, there is no discussion of privacy enhancing technologies, no discussion of the privacy risks to individual employees and no direction on mitigating those privacy risks. The expert advice we have obtained from industry leaders is what was relied on and that confirms the risk to the privacy of individual employees is a real one and warrants use of privacy enhancing technologies such as the web robot exclusion protocol. Unfortunately, there is no right of appeal from the refusal of a local authority to accept our recommendations in a privacy investigation report of the OIPC.

Investigation Report F-2012-001

(Saskatchewan Telecommunications)

Summary

This Investigation Report was issued August 27, 2012. The OIPC received a complaint regarding an apparent over collection of a customer's personal information by Saskatchewan Telecommunications (SaskTel) as part of its identity verification process. Though SaskTel eventually addressed the Complainant's concerns, the investigation continued as I had concerns with SaskTel's broader collection practices. This included consideration of the authority for SaskTel to collect from customers their Social Insurance number, their driver's license and the health services number/card particularly given the prohibition in section 11 of HIPA of any requirement to produce

the health services number for obtaining a non-health service related reason. I found that SaskTel did not have authority to collect the Saskatchewan health services number. Secondly, SaskTel did not provide a satisfactory explanation as to why it needed to collect other unique identifiers over the phone since it could not verify the accuracy of same. This part of the Report addresses in detail both identification and authentication and the differences between each exercise. Thirdly, I found that SaskTel was apparently collecting third party personal information without authority. This included a discussion of the duty to ensure personal information collected is "as accurate and complete as is reasonably possible." Also found was that SaskTel did not meet the notice requirements of section 26(2) of FOIP. I also considered the role of ExpressAddress but had insufficient information to determine whether this acted an information services management provider of SaskTel.

Recommendations and Response

I recommended that SaskTel conduct a PIA, revise its privacy policy and prepare a script to ensure that its customers understand what is optional when providing proof of identity. I recommended that SaskTel cease collecting its customers' unique identifiers unless it is able to establish the necessity of and its authority to collect it. I also recommended that SaskTel review its collection practices for purposes of determining credit worthiness to ensure it is keeping with the data minimization principle. I further recommended SaskTel within 60 days purge from its systems all personal information and personal health information of its customers and third parties collected without the requisite authority.

In the Report in paragraph [2], I referenced a request made to SaskTel for certain information "on or about February 27, 2007". SaskTel, subsequent to issue of the Report, advised that they had no record of receipt of such a communication from the OIPC. I then undertook a careful review of our complete investigation file. I found a document which appeared to be a copy of a letter to SaskTel dated February 27, 2007 from the OIPC. At the time our formal Report was prepared I assumed that this letter had been sent on or about February 27, 2007 and therefore referenced it in paragraph [2] in our Report. On my latest review of the file, I found another copy of the same document with a notation that suggests it may not have been sent. I have no reason to dispute the assertion of SaskTel that it did not receive such correspondence. I might also note however that, consistent with our usual practice, we provided SaskTel with our "decision letter" on April 12, 2012 which is our preliminary assessment of the evidence and submissions and our analysis. In that letter we included the statement: "On or about February 27, 2007, we asked SaskTel to provide a more detailed response to address the following...". We routinely provide this kind of preliminary advice to

ensure that every opportunity is given to the government institution to avoid a public report if there can be an agreement on remedial action. We also do this to avoid any surprises to the government institution and to ensure that the factual foundation for our analysis, findings and recommendations is accurate. When I reviewed our complete file in response to the SaskTel concern, I could find no evidence that SaskTel at any time in 2012 advised us that it did not have any knowledge of a February 27, 2007 communication from our office. Neither can I find on the file any protest or representation from SaskTel that the five questions enumerated by our office in the preliminary analysis had not been communicated to SaskTel on or about February 27, 2007. In those circumstances, we proceeded to issue our Investigation Report confident that the background section which appeared on page 1 of the April 12, 2012 document prepared by our office and shared with SaskTel was accurate. In fact that conclusion was in error. That does not, however, in any way, change our findings and recommendations which are recorded on page 57 and 58 of this Report.

My office received a response from SaskTel on September 24, 2012 indicating it would be following many of my recommendations. SaskTel did not agree to undertake a PIA as it claims to have conducted one on February 14, 2011. It stated that it undertakes PIAs on all projects as it is mandatory within its project management process. SaskTel did not comply with my recommendation to cease collecting health services numbers, but indicated it had already stopped collecting roommate information. SaskTel advised that it would comply with the remaining recommendations including reviewing its arrangement with ExpressAddress.

Financial Statements

For the Year Ended March 31, 2013

Saskatchewan
Information and Privacy
Commissioner

503 - 1801 Hamilton Street
Regina, Saskatchewan
S4P 4B4

Tel: (306) 787-8350
Fax: (306) 798-1603
Website: www.oipc.sk.ca

June 12, 2013

2012 - 2013 MANAGEMENT REPORT

The accompanying financial statements are the responsibility of management and have been approved in principle by the Office of the Information and Privacy Commissioner. The financial statements have been prepared in accordance with Canadian public sector accounting standards.

Management maintains appropriate systems of internal control, including policies and procedures which provide reasonable assurance that the Office's assets are safeguarded and that financial records are relevant and reliable.

The Provincial Auditor of Saskatchewan conducts an independent audit of the financial statements. Her examination is conducted in accordance with Canadian generally accepted auditing standards and includes tests and other procedures which allow her to report on the fairness of the financial statements.

R. Gary Dickson, Q.C.
Saskatchewan Information and

Pam Scott
Director of Operations

PROVINCIAL AUDITOR
of Saskatchewan

INDEPENDENT AUDITOR'S REPORT

To: The Members of the Legislative Assembly of Saskatchewan

I have audited the accompanying financial statements of the Office of the Information and Privacy Commissioner, which comprise the statement of financial position as at March 31, 2013 and the statements of operations and accumulated surplus, changes in net debt and cash flows for the year then ended, and a summary of significant accounting policies and other explanatory information.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these financial statements in accordance with Canadian public sector accounting standards and for such internal control as management determines is necessary to enable the preparation of financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

My responsibility is to express an opinion on these financial statements based on my audit. I conducted my audit in accordance with Canadian generally accepted auditing standards. Those standards require that I comply with ethical requirements and plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

I believe that the audit evidence I have obtained is sufficient and appropriate to provide a basis for my audit opinion.

Opinion

In my opinion, the financial statements present fairly, in all material respects, the financial position of the Office of Information and Privacy Commissioner as at March 31, 2013, the results of its operations, changes in its net debt and its cash flows for the year then ended in accordance with Canadian public sector accounting standards.

Regina, Saskatchewan
June 12, 2013

Bonnie Lysyk, MBA, CA
Provincial Auditor

1500 Chateau Tower - 1920 Broad Street - Regina, Saskatchewan - S4P 3V2
t 306.787.6398 f 306.787.6383 e info@auditorsk.ca
www.auditor.sk.ca

Office of the Information and Privacy Commissioner
Statement of Financial Position
As at March 31

	2013	2012
Financial assets		
Due from the General Revenue Fund	$ 24,382	$ 51,002
Accounts Receivable	4,130	-
	28,512	51,002
Liabilities		
Accounts payable	21,996	22,611
Accrued employee costs	6,516	28,391
	28,512	51,002
Net debt (Statement 3)	-	-
Non - financial assets		
Tangible capital assets (Note 3)	13,029	18,834
Prepaid expenses	13,569	17,823
	26,598	36,657
Accumulated surplus (Statement 2)	$ 26,598	$ 36,657

Contractual obligations (Note 8)

Office of the Information and Privacy Commissioner
Statement of Operations and Accumulated Surplus
For the Year Ended March 31

	Budget (Note 4)	2013 Actual	2012 Actual
Revenue			
General Revenue Fund Appropriation	$ 1,065,000	1,005,562	1,128,657
Miscellaneous Revenue	-	564	-
Total Revenue	1,065,000	1,006,126	1,128,657
Expenses			
Salaries and other employment expenses	$ 774,000	751,126	811,778
Administration and operating expenses	62,700	53,207	52,577
Rental of space and equipment	144,950	143,400	140,668
Travel	33,500	22,870	34,604
Advertising and promotion	8,700	4,346	10,618
Amortization	-	14,660	17,752
Contractual and legal services	41,150	26,576	53,675
Total Expenses	1,065,000	1,016,185	1,121,672
Operating Surplus (Deficit)	$ -	(10,059)	6,985
Accumulated surplus, beginning of year		36,657	29,672
Accumulated surplus, end of year (Statement 1)		$ 26,598	$ 36,657

Statement 3

Office of the Information and Privacy Commissioner
Statement of Changes in Net Debt
For the Year Ended March 31

	2013	2012
Operating surplus (deficit)	$ (10,059)	$ 6,985
Acquisition of tangible capital assets	(8,855)	(8,897)
Amortization of tangible capital assets	14,660	17,752
	5,805	8,855
Increase (decrease) in prepaid expense	4,254	(15,840)
	10,059	(6,985)
Decrease (Increase) in net debt	-	-
Net debt, beginning of year	-	-
Net debt, end of year (Statement 1)	$ -	$ -

Office of the Information and Privacy Commissioner
Statement of Cash Flows
For the Year Ended March 31

Cash from (used in) operating activities:	**2013**	**2012**
General Revenue Fund appropriation received	$ 1,028,616	$ 1,103,878
Salaries paid	(773,001)	(788,887)
Supplies and other expenses paid	(246,760)	(306,094)
Cash from (used in) operating activities	8,855	8,897
Cash from (used in) in capital activities:		
Purchase of tangible capital assets	(8,855)	(8,897)
Cash from (used in) capital activities	(8,855)	(8,897)
Increase (decrease) in cash and cash equivalents	-	-
Cash and cash equivalents, beginning of year	-	-
Cash and cash equivalents, end of year	$ -	$ -

Notes to the Financial Statements

1. Authority and Description of Operations

The Freedom of Information and Protection of Privacy Act (Act) states that the Lieutenant Governor in Council, on the recommendation of the Assembly, shall appoint an Information and Privacy Commissioner. The Commissioner is an officer of the Legislative Assembly and is appointed by resolution. The mandate of the Office of the Information and Privacy Commissioner (Office) is to review Government decisions under the Act to ensure the protection of the public's right to access records held or controlled by the Government and to ensure that personal information is only collected, used and disclosed according to the manner and purposes set out in the Act.

2. Significant Accounting Policies

The Office uses Canadian public sector accounting standards to prepare its financial statements. These statements do not include a Statement of Remeasurement gains or losses as the Office has no activities that give rise to remeasurement gains or losses. As a result, the accumulated surplus is the same as its accumulated operating surplus. The following accounting policies are considered to be significant.

(a) Revenue

The Office receives an appropriation from the General Revenue Fund to carry out its work. General Revenue Fund appropriations are included in revenue when amounts are spent or committed.

(b) Tangible capital assets

Tangible capital assets are reported at cost less accumulated amortization. Tangible capital assets are amortized on a straight-line basis over a life of three to five years.

(c) Application of New Accounting Standards

Effective April 1, 2012, the Office applied the following standards on a prospective basis. The application of these standards have had no effect on these financial statements.

i) PS1201 - Financial Statement Presentation

ii) PS2601 - Foreign Currency Translation

iii) PS3450 - Financial Instruments

3. Tangible Capital Assets

	2013				
	Hardware & Software	Equipment & Furniture	Leasehold Improvements	Total 2013	Total 2012
Cost, April 1	$ 87,982	$ 131,945	$ 43,852	$ 263,779	254,882
Additions	7,085	1,071	699	8,855	8,897
Disposals	(26,486)	(3,094)	-	(29,580)	-
Cost, March 31	68,581	129,922	44,551	243,054	263,779
Accumulated Amortization, April 1	77,951	123,142	43,852	244,945	227,193
Annual Amortization	7,281	7,239	140	14,660	17,752
Adjustment for disposals	(26,486)	(3,094)	-	(29,580)	-
Accumulated Amortization, March 31	58,746	127,287	43,992	230,025	244,945
Net Book Value, March 31	$ 9,835	$ 2,635	$ 559	$ 13,029	18,834

4. Budget

These amounts represent funds approved by the Legislative Assembly to enable the Office to carry out duties under *The Freedom of Information and Protection of Privacy Act*. The Office's expenditures are limited to the amount appropriated to it by the Legislative Assembly.

5. Lapsing of Appropriation

The Office follows *The Financial Administration Act, 1993* with regards to its spending. If the Office spends less than its appropriation by March 31, the difference is not available to acquire goods and services in the next fiscal year.

6. Costs Borne by Other Agencies

The Office has not been charged with certain administrative costs and employee benefit costs. These costs are borne by the Legislative Assembly and the Ministry of Finance. No provision for these costs is reflected in these financial statements.

7. Financial Instruments

The Office's financial instruments include Due from the General Revenue Fund, Accounts payable and Accrued employee payables. The carrying amount of these instruments approximates fair value due to their immediate or short-term maturity. These instruments have no significant interest rate and credit risk.

8. Contractual Obligations

During the year ended March 31, 2011, the Office and its landlord made a new lease whereby the Office agreed to rent the premises for five years commencing June 30, 2010. Annual lease payments are $138,977 before escalation adjustments.

9. Pension Plan

The Office participates in a defined contribution pension plan for the benefit of its employees. The Office's financial obligation of the plan is limited to making payments of 5% of employees' salaries for current service.

Appendices

Appendix 1
Requests for Review Opened in 2012-2013

Requests for Review Opened in 2012 - 2013 Fiscal Year	
Name of Agency	Number of Request for Reviews Opened
Automobile Injury Appeal Commission	1
City of Regina	2
Financial and Consumer Affairs Authority	1
Government Relations	1
Information Services Corporation	1
Mamawetan Churchill River Regional Health Authority	1
Ministry of Economy	1
Ministry of Environment	1
Ministry of Finance	1
Ministry of Health	2
Ministry of Justice	3
Ministry of Labour Relations and Workplace Safety	1
RMs, Villages and Towns	5
Saskatchewan Human Rights Commission	1
Saskatchewan Labour Relations Board	1
Saskatoon Regional Health Authority	1
Saskatchewan Telecommunications	10
School Divisions	2
Saskatchewan Government Insurance	3
Tourism Saskatchewan	1
University of Regina	3
Saskatchewan Workers' Compensation Board	2

Appendix 2
Requests for Review Closed in 2012-2013

Requests for Review Closed in 2012 - 2013 Fiscal Year	
Name of Agency	Number of Request for Reviews Closed
Automobile Injury Appeal Commission	1
City of Regina	4
City of Saskatoon	1
Executive Council	1
Heartland Regional Health Authority	1
Kelsey Trail Regional Health Authority	1
Mamawetan Regional Health Authority	1
Ministry of Advanced Education	1
Ministry of Agriculture	2
Ministry of Central Services	1
Ministry of Economy	1
Ministry of Environment	3
Ministry of Health	2
Ministry of Justice	9
Ministry of Social Services	4
Physicians	2
Prince Albert Parkland Regional Health Authority	1
Regina Public Library	1
Regina Qu'Appelle Regional Health Authority	1
RMs, Villages and Towns	3
Saskatchewan Crop Insurance Corporation	1
Saskatchewan Highway Traffic Board	1

Requests for Review Closed in 2012 - 2013 Fiscal Year	
Name of Agency	Number of Request for Reviews Closed
Saskatchewan Human Rights Commission	1
Saskatchewan Labour Relations Board	1
SaskEnergy	1
SaskPower	1
Saskatchewan Telecommunications	9
School Divisions	3
Saskatchewan Government Insurance	4
Saskatchewan Institute of Applied Science & Technology	2
Sunrise Regional Health Authority	1
Tourism Saskatchewan	1
University of Regina	1
University of Saskatchewan	2
Saskatchewan Workers' Compensation Board	4
Other	1

Appendix 3
Definitions

The following is a list of definitions of terms or abbreviations used in the course of this document or referenced in documents accessible from the website: www.oipc.sk.ca.

Additional definitions are found in the three provincial statutes: *The Freedom of Information and Protection of Privacy Act* (FOIP), *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) and *The Health Information Protection Act* (HIPA).

Applicant refers to an individual who has made an access request to a government institution, local authority, or health information trustee.

Access is the right of an individual (or his or her lawfully authorized representative) to view or obtain copies of records in the possession or control of a government institution, local authority or trustee including his/or her personal information/ personal health information.

Collection is defined by HIPA as to "gather, obtain access to, acquire, receive or obtain personal health information from any source by any means" (section 2(b) of HIPA).

Commissioner refers to the Saskatchewan Information and Privacy Commissioner.

Complainant refers to an aggrieved individual who makes a formal complaint to the Commissioner to investigate an alleged breach of privacy by that public body or trustee pursuant to sections 33 of FOIP, 32 of LA FOIP, or 52 of HIPA.

Complaint is written concern that there has been a breach of privacy by a government institution, local authority or trustee.

Confidentiality is the protection of personal information and personal health information once obtained against improper or unauthorized use or disclosure. This is just one aspect of privacy and is not synonymous with 'privacy'.

Control is a term used to indicate that the records in question are not in the physical possession of the public body or trustee, yet still within the influence of that body via another mechanism (e.g. contracted service).

Custody is the physical possession of a record by a public body or trustee.

Detailed Research and Commentary refers to requests for evaluative, general, non-binding advice that take in excess of one hour of research, most of these would involve in excess of four hours research.

Disclosure is sharing of personal information with a separate entity, not a division or branch of the public body or trustee in possession or control of that record/ information.

Duty to Assist means responding openly, accurately and completely to an individual requesting access to records in the possession or control of a government institution or local authority or to personal health information in the custody or control of a health information trustee.

Exclusions are prescribed records and organizations that are not subject to FOIP, LA FOIP or HIPA.

Exemptions are sections of the relevant statutes referenced to justify the denial of access to records by the individual either for mandatory or discretionary reasons.

FOIP refers to *The Freedom of Information and Protection of Privacy Act* that came into force in 1992.

FOIP Coordinator refers to an individual designated pursuant to section 60 of FOIP for managing access and privacy issues in any public body with this title.

FOIP Regime means the statute, regulations, as well as the policies, practices and procedures for the implementation of the statute and regulations.

Government Institution refers to those public bodies prescribed in FOIP and the FOIP Regulations and includes approximately 90 provincial government departments, agencies, and Crown corporations.

Head of a public body is the individual accountable by law for making the final decision on access requests, but may delegate these powers to someone else in the organization. This is typically the Minister of a ministry, the mayor of a municipality and the CEO of a local authority or Crown corporation.

HIPA refers to *The Health Information Protection Act* that came into force in 2003.

Identity Theft occurs when one person uses another's personal information without his/her knowledge or consent to commit a crime such as fraud or theft.

LA FOIP refers to *The Local Authority Freedom of Information and Protection of Privacy Act* that came into force in 1993.

Local Authorities means local government including library boards, municipalities, regional colleges, schools, universities, and regional health authorities as prescribed by LA FOIP and the LA FOIP Regulations.

Mediation is the process of facilitating discussion between the parties involved in a review or investigation by the OIPC with the goal of negotiating a mutually acceptable resolution to the dispute without the issuance of a formal report.

OIPC is an abbreviation for the Office of the Saskatchewan Information and Privacy Commissioner.

Personal Information is "recorded information about an identifiable individual" and includes details such as your name, address, phone number, SIN, race, driver's license number, health card number, credit ratings, and opinions of another person about you.

Personal Health Information includes information about your physical or mental health and/or information gathered in the course of providing health services for you.

PIA is an abbreviation for a Privacy Impact Assessment. A PIA is a diagnostic tool designed to help organizations assess their compliance with the privacy requirements of Saskatchewan legislation.

Privacy, in terms of 'information privacy,' means the right of the individual to determine when, how and to what extent he/she will share information about him/herself with others. Privacy captures both security and confidentiality of personal information/personal health information.

Privacy Breach happens when there is an unauthorized collection, use or disclosure of personal information/personal health information regardless of whether the information ends up in a third party's possession.

Public Bodies are organizations in the public sector including government institutions and local authorities.

Record is information in any form or format and includes such items as documents, maps, books, post-it notes, handwritten notes, phone messages, photographs, and tape recordings.

Report is a document prepared by the Saskatchewan Information and Privacy Commissioner that issues recommendations to a public body for changes and/or actions in response to the findings of a formal access review or breach of privacy complaint.

Research is the systematic investigation designed to develop or establish principles, facts or generalizable knowledge.

Review is the process by which the OIPC considers either a decision or failure of a trustee to provide an applicant with access to his or her personal health information.

Secondary Purpose refers to the use or disclosure of personal information/personal health information for a purpose other than that for which it was originally collected.

Security refers to steps taken to protect personal information or personal health information from unauthorized disclosure.

Severing is the exercise by which portions of a document are blacked out pursuant to section 8 of FOIP, section 8 of LA FOIP or section 38(1) of HIPA before that document is provided to an applicant.

Summary advice refers to requests for information received from public bodies, trustees or the public that can be responded to with less than one hour of research.

Surrogate refers to someone other than the individual but who is exercising rights or powers under section 59 of FOIP, section 49 of LA FOIP or section 56 of HIPA on behalf of the individual.

Third Party is a person other than the applicant or a public body.

Trustees as defined within section 2(t) of HIPA are individuals and corporations who are part of Saskatchewan's health system in custody or control of personal health information and any government institution as defined by FOIP.

Use indicates the internal utilization of personal information by a public body and includes sharing of the personal information in such a way that it remains under the control of that public body.

Appendix 4
Sample List of Presentations

Made From April 1, 2012 to March 31, 2013

- Canada Health Infoway Privacy Forum
- Canada's Public Guardians and Public Trustees Annual Meeting
- Canadian Bar Association - Labour and Administrative Law Section meeting (Saskatchewan South)
- Canadian Bar Association - Privacy and Access Law Section meeting (Saskatchewan South)
- Canadian Industrial Relations Association
- Community Agencies and Schools Supporting Youth conference
- Health Information Privacy Security Summit
- Health Sector Access and Privacy Forum
- Lorman Education Services - Medical Records Law in Saskatchewan
- National Association for Information Destruction—Data Destruction Policy and Training Development workshop
- Office of the Advocate for Children and Youth
- Saskatchewan Access, Privacy, Security and Records Management Forum (Ministry of Justice, Access and Privacy Branch)
- Saskatchewan Association of Licensed Practical Nurses
- Saskatchewan Early Childhood Association conference
- Saskatchewan Legislative Internship Program
- Saskatchewan Registered Nurses Association - Investigation Committee
- Saskatchewan School Board Association
- Saskatchewan 3.0 Summit
- University of Alberta Access and Privacy Conference
- University of Saskatchewan, College of Law and Johnson-Shoyama Graduate School of Public Policy
- Western Canada Health Information Privacy Symposium

Appendix 5
List of Bodies Subject to OIPC Oversight

Government Institutions

- Ministries (15)
- Agencies, Boards and Commissions (30)
- Crown Corporations (22)

Local Authorities

- Libraries (500 +)
- Municipalities (786)
  - urban municipalities (466)
  - rural municipalities (296)
- Regional Colleges (7)
- Regional Health Authorities (13)
- School Divisions (28)
- SIAST (4 campuses)
- Universities (2)

Health Information Trustees

- Regional Health Authorities (13) and Affiliates
- Regulated Health Professions
  - includes physicians, surgeons and registered nurses
- Self-Regulating Health Professional Associations (27)
- Pharmacies
- Ambulance Operators
- Community Clinics
- Government Institutions
- Personal Care Homes
- Mental Health Facilities
- Laboratories
- Saskatchewan Cancer Agency